# Guía de seguridad TIC
# CCN-STIC 888A

# Guía de configuración segura para Google WorkSpace


Septiembre 2021

**Catálogo de Publicaciones de la Administración General del Estado**
**https://cpage.mpr.gob.es**

Edita:

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-21-166-X

Fecha de Edición: septiembre de 2021
Davinci Tecnologías de la Información, S.L ha participado en la realización y modificación del presente documento y sus anexos, que ha sido financiado por Google. Sidertia Solutions S.L. ha participado en la revisión de esta guía.

# PRÓLOGO

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN)

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

Septiembre de 2021



Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

# ÍNDICE

# 1. GUÍA DE CONFIGURACIÓN SEGURA PARA GOOGLE WORKSPACE

## 1.1 Descripción del uso de esta guía

El objetivo de la presente guía es documentar y ayudar al usuario a configurar un entorno de Google Workspace (GW) con el correcto cumplimiento de los requisitos expuestos en el Esquema Nacional de Seguridad en su categoría ALTA.

En esta guía se abordarán los servicios incluidos en Google Workspace en el cual se incluyen la solución ofimática de Google, la solución de correo electrónico Gmail y el servicio de alojamiento en la nube de Google Drive entre muchos otros.

## 1.2 Definición de la solución

Google Workspace es un conjunto de aplicaciones y servicios basados en la nube alojados en Google Cloud, propiedad de Google y disponibles desde todos los dispositivos con conexión a Internet. Google Workspace consiste en una plataforma en la que todos los productos de trabajo y productividad de Google están integrados en un único sistema que permite mejorar la comunicación y gestión de las actividades entre distintos colaboradores.


*Figura 1. Logo de Google WorkSpace*

Dentro de esta solución encontramos los siguientes servicios disponibles:

- Gmail: Servicio de correo electrónico.
- Drive: Servicio de alojamiento de archivos en la nube.
- Meet: Servicio de videotelefonía.
- Calendar: Agenda y calendario electrónico.
- Chat: Software de comunicación.
- Currents: Software para la comunicación empresarial interna.
- Jamboard: Pizarra digital.

- Docs, Sheet, Slides: Software de ofimática.
- Keep: Software que permite organizar la información personal a través de archivos de notas.
- Sites: Herramienta para la creación de páginas web.
- Forms: Software de administración de encuestas.
- Apps Script: Herramienta para la creación de scripts y automatizaciones.
- Cloud Search: Herramienta para realizar búsquedas a través de GW.

Google Workspace presenta tres productos distintos a contratar. Esta guía se basa en el plan Enterprise, que es el que más se ajusta al cumplimiento de todas las medidas del ENS, y además es el más recomendado para entornos que precisen el nivel ALTO.

En la siguiente tabla se presenta la comparativa en medidas de seguridad entre las diferentes ediciones:

| Seguridad y protección de datos | Business Starter | Business Standard | Business Plus | Enterprise |
|---|---|---|---|---|
| Verificación en dos pasos | ✓ | ✓ | ✓ | ✓ |
| Llaves de seguridad para la verificación en dos pasos | ✓ | ✓ | ✓ | ✓ |
| Uso obligatorio de conexiones SSL | ✓ | ✓ | ✓ | ✓ |
| Centro de alertas: notificaciones de posibles problemas de seguridad | ✓ | ✓ | ✓ | ✓ |
| Supervisión y control de la seguridad de las contraseñas | ✓ | ✓ | ✓ | ✓ |
| Colaboración con dominios externos de confianza | | ✓ | ✓ | ✓ |
| Configurar la duración de las sesiones de los servicios de Google | | | ✓ | ✓ |
| Control de acceso contextual | | | | ✓ |
| Centro de seguridad | | | | ✓ |
| Regiones de datos | | | | ✓ |

| Informes y registros de auditoría | Business Starter | Business Standard | Business Plus | Enterprise |
|---|---|---|---|---|
| Tendencias de uso de las aplicaciones y los usuarios | ✓ | ✓ | ✓ | ✓ |
| Registros de auditoría de la actividad de usuarios y administradores | ✓ | ✓ | ✓ | ✓ |
| Funciones avanzadas de auditoría e informes de Drive | | ✓ | ✓ | ✓ |
| Informes de asistencia de Google Meet | | | ✓ | ✓ |

| Integración de aplicaciones de terceros | Business Starter | Business Standard | Business Plus | Enterprise |
|---|---|---|---|---|
| Inicio de sesión único (SSO) con Google como proveedor de identidades | ✓ | ✓ | ✓ | ✓ |
| Inicio de sesión único (SSO) con un proveedor de identidades externo | ✓ | ✓ | ✓ | ✓ |
| Catálogo de aplicaciones con más de 200 aplicaciones SAML preconfiguradas | ✓ | ✓ | ✓ | ✓ |
| Aprovisionamiento automático de aplicaciones SAML (número máximo) | 3 | 3 | 3 | 3 |
| LDAP seguro: conectar aplicaciones y servicios basados en LDAP | | | ✓ | ✓ |
| Prevención de la pérdida de datos (DLP) | | | | ✓ |

| Gestión de dispositivos | Business Starter | Business Standard | Business Plus | Enterprise |
|---|---|---|---|---|
| Gestión básica de puntos finales (muchas funciones) | | ✓ | ✓ | ✓ |
| Gestión de aplicaciones Android | | | ✓ | ✓ |
| Gestión avanzada de puntos finales (muchas funciones) | | | ✓ | ✓ |
| Distribuir aplicaciones móviles de forma selectiva | | | ✓ | ✓ |
| Registro de auditoría de dispositivos | | | ✓ | ✓ |
| Informe sobre los dispositivos inactivos propiedad de la empresa | | | ✓ | ✓ |
| Dispositivos Android propiedad de la empresa | | | ✓ | ✓ |

| Drive y editores de Documentos | Business Starter | Business Standard | Business Plus | Enterprise |
|---|---|---|---|---|
| Activar o desactivar la opción de crear Documentos | ✓ | ✓ | ✓ | ✓ |
| Unidades compartidas para equipos | | ✓ | ✓ | ✓ |
| Funciones avanzadas de auditoría e informes de Drive (registro de auditoría de Drive) | | ✓ | ✓ | ✓ |
| Permisos avanzados de Drive para compartir archivos | | ✓ | ✓ | ✓ |
| Gestionar aprobaciones de documentos | | ✓ | ✓ | ✓ |

| | | | | |
|---|---|---|---|---|
| Gestionar metadatos de Drive (etiquetas y campos personalizados) | | ✓ | ✓ | ✓ |
| Branding de la organización (plantillas personalizadas) | | ✓ | ✓ | ✓ |

# 2. CONFIGURACIÓN DE GOOGLE WORKSPACE

## 2.1 MARCO OPERACIONAL

### 2.1.1 Control de Acceso

El control de acceso comprende el conjunto de actividades que permiten o deniegan a una entidad, usuario o proceso, el acceso a un recurso del sistema para la realización de una acción concreta.

#### 2.1.1.1 Identificación

Para el acceso a Google Workspace se utilizan las cuentas de usuario de Google, asociadas a la organización. Dentro de la organización se pueden encontrar tres tipos de usuarios: superadministrador, administrador y usuario. La principal diferencia entre un superadministrador y un administrador es que los superadministradores tienen acceso a todas las funciones de la consola, mientras que el administrador solamente a una parte concreta, por ejemplo, el administrador de grupos, el cual tendría privilegios de administración solamente a la parte de creación y modificación de grupos de usuarios. Es recomendable tener al menos dos superadministradores en la organización, de esta forma, si uno se olvida de la contraseña, el otro podrá recuperarla.

Google Workspace permite además sincronizar las cuentas de Microsoft Active Directory o de un servidor LDAP usando Google Cloud Directory Sync (GCDS). También tiene la posibilidad de sincronizar solo las contraseñas de los usuarios de Microsoft Active Directory, usando G Suite Password Sync (GSPS).

**Google Cloud Directory Sync**

Con Google Cloud Directory Sync, se puede sincronizar los datos de la cuenta de Google con Microsoft Active Directory o un servidor LDAP. GCDS no migra ningún contenido (como mensajes de correo electrónico, eventos de calendario o archivos) a la cuenta de Google. Se puede usar GCDS para sincronizar los usuarios, grupos y contactos compartidos de Google de forma que coincidan con la información que figura en el servidor LDAP.

Su funcionamiento es el siguiente:
En primer lugar, se configuran unas reglas para especificar cómo el sistema genera una lista con los datos. Durante una sincronización, la lista se exporta desde el servidor LDAP.

GCDS se conecta a la cuenta de Google y genera una lista con los usuarios, grupos y contactos compartidos que se especifiquen.

A continuación, GCDS compara estas listas y actualiza la cuenta de Google para hacer coincidir los datos. Una vez que se complete la sincronización, se recibe un informe por correo electrónico para poder monitorizar el proceso.

Para la implementación de esta herramienta, puedes seguir la siguiente guía del fabricante:
https://cloud.google.com/solutions/federating-gcp-with-active-directory-synchronizing-user-accounts?hl=es#configuring_active_directory_synchronization

**G Suite Password Sync**

G Suite Password Sync (GSPS) sincroniza automáticamente las contraseñas de Google Workspace de los usuarios con las de Microsoft Active Directory. Cuando se cambia la contraseña de Active Directory de un usuario, GSPS implementa el cambio en la cuenta de Google gestionada de forma inmediata.

GSPS nunca cambia las contraseñas de Active Directory, solo sincroniza los cambios de contraseña de Active Directory con la cuenta de Google de la organización.

Para la implementación de esta herramienta, puedes seguir la siguiente guía del fabricante:
https://support.google.com/a/answer/2611842?hl=es

Para la gestión de las cuentas de usuario, de acuerdo con las exigencias del Esquema Nacional de Seguridad, se deberá seguir los siguientes puntos:

- Cada cuenta estará asociada a un identificador único. Cuando un usuario tenga diferentes roles, recibirá identificadores únicos por cada rol.
- Cada entidad que acceda al sistema contará con un identificador único que permita posteriormente identificar de manera sencilla y hacer una traza de roles que dispone y acciones que ha ejecutado.
- Las cuentas deben ser inhabilitadas en los siguientes casos: cuando el usuario deja la organización; cuando el usuario cesa en la función para la cual se requería la cuenta de usuario; o, cuando la persona que la autorizó da orden en sentido contrario. Adicionalmente las cuentas deben quedar bloqueadas al superar el número máximo de intentos de inicio de sesión, cumpliendo así con lo expuesto en el ENS.

**Cuentas de usuario**

Para las cuentas de usuario se deberán de aplicar una serie de acciones recomendadas que las mantenga seguras de ataques externos:

- Se deberá aplicar la verificación en dos pasos de manera obligatoria.
- Se deberá aplicar la política de contraseñas únicas, es decir, no usar la misma contraseña en cuentas diferentes, ya sean de la misma organización o de servicios externos a la misma.
- Se deberá activar las alertas de actividad en las cuentas para supervisar la actividad de las mismas.
- En caso de sospecha de que se ha vulnerado una cuenta, se deberá revisar los dispositivos asociados a la cuenta y evaluar la exposición de la misma, así como la comprobación de si se ha configurado algún ajuste malicioso.

Para la implementación de las medidas y buenas prácticas de seguridad comentadas anteriormente, puede consultar la web del fabricante:

| Descripción medida | URL |
|---|---|
| Aplicar la verificación en dos pasos obligatoria para los usuarios. | https://support.google.com/a/answer/9176657?hl=es&ref_topic=2759193 |
| Usar contraseñas únicas. | https://support.google.com/accounts/answer/9094506?hl=es |
| Configurar alertas de actividad. | https://support.google.com/a/answer/3230421 |
| Identificar y proteger cuentas vulneradas | https://support.google.com/a/answer/2984349#zippy=%2Cpaso-suspender-temporalmente-la-cuenta-de-usuario-sospechosa%2Cpaso-investigar-la-cuenta-para-detectar-actividad-no-autorizada%2Cpaso-revocar-el-acceso-a-la-cuenta-afectada%2Cpaso-volver-a-dar-acceso-al-usuario%2Cpaso-registrarse-en-la-verificaci%C3%B3n-en-dos-pasos-con-llaves-de-seguridad%2Cpaso-a%C3%B1adir-proteger-o-editar-las-opciones-de-recuperaci%C3%B3n%2Cpaso-habilitar-las-alertas-de-actividad-de-la-cuenta |

Puede encontrar más información sobre la implementación de las medidas y buenas prácticas de seguridad en la siguiente guía del fabricante: https://support.google.com/a/answer/7587183?hl=es#zippy=%2Caccounts%2Ccuentas

**Cuentas de Administrador**

Además de las recomendaciones generales para la protección de las cuentas de usuario, para las cuentas de administración se deberán tener en cuenta más recomendaciones.

Las cuentas de administrador controlan el acceso a todos los datos corporativos y de empleados de la organización, por lo que es especialmente importante que las cuentas estén protegidas, para ello se deberán realizar las siguientes acciones:

- Se deberá crear una cuenta de administrador por cada super administrador, cada una de ellas gestionada por una persona diferente.
- Control activo de la consola de administración de Google para ver el historial de las tareas realizadas por cada cuenta de administrador.

- Se deberá generar un código de seguridad para que en caso de pérdida de contraseña o de la clave de la doble verificación se permita recuperar la cuenta. Esta clave deberá ser guardada en un lugar seguro.
- Las cuentas de administradores se deberán usar solo para realizar tareas que requieren de un super administrador.

Para la implementación de las medidas y buenas prácticas de seguridad comentadas anteriormente, puede consultar la web del fabricante:

| Descripción medida | URL |
|---|---|
| Crear cuentas de superadministrador distintas | https://support.google.com/a/answer/9011373#zippy=%2Cconfigurar-varias-cuentas-de-superadministrador |
| Revisar el registro de auditoría de la consola de administración. | https://support.google.com/a/answer/4579579 |
| Guardar códigos de seguridad con antelación | https://support.google.com/accounts/answer/1187538?hl=es |
| No llevar a cabo actividades rutinarias con cuentas de superadministrador. | https://support.google.com/a/answer/9011373#zippy=%2Cno-utilizar-cuentas-de-superadministrador-para-llevar-a-cabo-actividades-rutinarias |

Puede encontrar más información sobre la implementación de las medidas y buenas prácticas de seguridad en la siguiente guía del fabricante: https://support.google.com/a/answer/7587183?hl=es#zippy=%2Caccounts%2Cadministrador

#### 2.1.1.2 Requisitos de acceso

El ENS especifica en el control de requisitos de acceso que los recursos del sistema se protegerán con algún mecanismo que impida su utilización, salvo a las entidades que disfruten de derechos de acceso suficientes. Deberán administrarse permisos para controlar el acceso a las identidades de personas que requieren acceso a GW y sus servicios. Los permisos controlan quién puede acceder a qué y en qué condiciones. Los permisos para identidades humanas específicas se deberán establecer para otorgar acceso a acciones de servicio específicas en recursos específicos. Además, deberán especificarse las condiciones que deben cumplirse para que se otorgue el acceso.

Dentro de GW la forma más sencilla de dar privilegios de administrador a otro usuario es asignándole roles de administrador predefinidos. Cada rol concede privilegios con los que, de forma conjunta, se puede realizar una tarea empresarial habitual. Por ejemplo, con un rol se pueden gestionar cuentas de usuario; con otro, grupos; con otro distinto, calendarios y recursos, y así sucesivamente. También permite crear un rol de administrador personalizado para asignar privilegios concretos a algunos usuarios. Los roles personalizados permiten incluir privilegios de administrador que permitan completar determinadas tareas de gestión en la consola de administración de Google.

Puede encontrar más información sobre la implementación de los roles personalizados en la siguiente guía del fabricante:
https://support.google.com/a/answer/2406043

También puedes consultar los roles predefinidos por GW en la siguiente web del fabricante:
https://support.google.com/a/answer/2405986?hl=es-419

- ❑ Se recomienda deshabilitar servicios adicionales a Google Workspace que no se utilizarán por los usuarios (por ejemplo, YouTube, Maps o Blogger).

De base toda organización creada en GW, dispone de un nivel organizativo superior, que engloba a todas las cuentas y dispositivos de la organización. Bajo ese nivel, se pueden añadir unidades organizativas, ya sean al mismo nivel o como una estructura jerarquizada. Las unidades organizativas (OU) en GW son estructuras lógicas que permiten agrupar cuentas de usuarios o dispositivos y aplicar sobre ellos determinados criterios de funcionamiento. Estas unidades organizativas solo pueden ser creadas por administradores de la organización. Dentro de estas unidades organizativas se pueden crear unidades organizativas secundarias las cuales heredan los ajustes de sus unidades superiores. Estos ajustes heredados pueden ser personalizados en las unidades organizativas hijas.

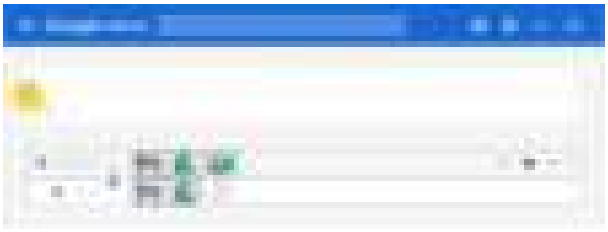

*figura 2. Ejemplo unidades organizativas*

Como se puede observar en la figura 2, los usuarios a nivel organizativo pueden usar Gmail, Google Drive y Google Meet, sin embargo, los usuarios de la unidad organizativa secundaria heredan solo permisos para Gmail y Google Drive.

- Se deberán crear unidades organizativas distintas para usuarios y dispositivos. De esta forma, se podrán personalizar los ajustes de los dispositivos y los usuarios gestionados según sea necesario.

Para la implementación de estas unidades organizativas, puede consultar la guía del fabricante:
https://support.google.com/a/answer/182537?hl=es

**Inicio de sesión único (SSO)**

Con el SSO, los usuarios solo tienen que iniciar sesión una vez para acceder a todas sus aplicaciones empresariales en la nube. Cuando esta función está configurada, los

usuarios pueden iniciar sesión en su proveedor de identidades (IdP) externo y acceder a las aplicaciones de Google directamente (sin necesidad de iniciar sesión por segunda vez).

Google ofrece un servicio de inicio de sesión único (SSO) basado en SAML. SAML es un estándar XML con el que los dominios web seguros pueden intercambiar datos de autenticación y autorización de los usuarios. Mediante SAML, un proveedor de servicios online puede ponerse en contacto con un proveedor de identidades online para que autentique a los usuarios que intenten acceder a contenido seguro.
Google utiliza SAML para confirmar la identidad del usuario. Esta confirmación solo aparece una vez en cada cuenta de un dispositivo. Una vez que el usuario confirme su identidad en un navegador Chrome o un dispositivo específico, se le puede permitir que vuelva a iniciar sesión sin que confirme de nuevo su identidad, ya que esto no supone un riesgo para la seguridad.

Para hacer uso del SSO de Google en aplicaciones externas, se adjunta la guía del fabricante:
https://support.google.com/a/answer/6087519?hl=es-419

**Acceso de terceros**

A la hora de iniciar sesión en aplicaciones externas con el SSO de Google, se deberá tener en cuenta las siguientes recomendaciones de seguridad:

- Se deberá revisar el acceso de las aplicaciones de terceros a los servicios principales de Google Workspace y decidir el uso de las mismas.

Para la implementación de este punto se deberá seguir la guía del fabricante:
https://support.google.com/a/answer/7281227?hl=es#zippy=%2Crevisar-las-aplicaciones-de-terceros-presentes-en-tu-entorno

- Se deberá crear una lista de aplicaciones de confianza que incluya las aplicaciones de terceros que puedan acceder a los servicios principales de Google Workspace.

Para la implementación de este punto se deberá seguir la guía del fabricante:
https://support.google.com/a/answer/7281227?hl=es#zippy=%2Cgestionar-el-acceso-de-las-aplicaciones-de-confianza-con-acceso-restringido-o-bloqueadas

#### 2.1.1.3 Proceso de gestión de derechos de acceso

A la hora de asignar roles es importante seguir la regla del mínimo privilegio, la cual nos indica que los privilegios de cada usuario se tienen que reducir al mínimo, es decir, parte de la premisa de otorgar los permisos necesarios y suficientes a un usuario para desempeñar sus actividades, por un tiempo limitado, y con el mínimo de derechos necesarios para sus tareas. De esta forma se acotan los daños que pudiera causar un usuario, de forma accidental o intencionada.

Como administrador de los servicios de Google Workspace de la organización, se pueden ver todos los roles y privilegios de administrador que tienen asignados los usuarios. Esta información puede ayudar a saber rápidamente qué nivel de acceso de administrador tiene un usuario en la cuenta y los servicios de Google Workspace de la organización. Para revisar las cuentas es necesario hacerlo desde una cuenta de administrador.

El propio fabricante nos recomienda una serie de buenas prácticas a la hora de gestionar las cuentas de la organización:

- Se deberá usar la menor cantidad de cuentas posible, pero tantas como sea necesario.
- Se deberán usar cuentas diferentes para la etapa de pruebas y de producción. Se crearán algunos usuarios para la etapa de pruebas que los administradores puedan usar para verificar los cambios de la configuración.

#### 2.1.1.4 Mecanismos de autenticación

Los mecanismos de inicio de sesión por parte de los usuarios han de ser robustos. Se debe aplicar una longitud mínima de contraseña y formar a los usuarios para evitar contraseñas comunes o reutilizadas. Para ello se deben seguir una serie de reglas que garanticen que la contraseña es segura:

- Utilizar una larga cadena de caracteres de diferentes tipos, como letras mayúsculas, minúsculas, números y caracteres especiales aumentando la entropía de la contraseña.
- No utilizar contraseñas comunes, como “123456” o “password”.
- No incluir el nombre del usuario dentro de la contraseña.
- El Esquema Nacional de Seguridad exige el uso de dos factores de autenticación para las categorías Medio y Alto. Esta autenticación multifactor o MFA se puede implementar en el servicio de Google Workspace de manera obligatoria.

Para la implementación de la medida puede consultar la guía del fabricante:
https://support.google.com/a/answer/9176657


*figura 3. Informe de seguimiento y control del registro de usuarios con autenticación multifactor*

Google Workspace exigirá el código MFA cuando se autentiquen los usuarios.

Para la autenticación en dos pasos, Google Workspace consta de varios métodos para cumplir la norma:

- Llaves de seguridad: Las llaves de seguridad son el método de verificación en dos pasos más seguro y protegen frente a amenazas de suplantación de identidad (phishing).
- Mensaje de Google: Se pueden configurar los dispositivos móviles Android o Apple para recibir mensajes de inicio de sesión. De este modo, cuando inicien sesión en la cuenta de Google desde su ordenador, se mostrará el mensaje "¿Estás intentando iniciar sesión?" en su dispositivo móvil.
- Google Authenticator y otros generadores de códigos de verificación: Los usuarios generan un código de verificación de un solo uso en un token de hardware (un pequeño dispositivo) o en una aplicación de su dispositivo móvil, como Google Authenticator. A continuación, se introduce el código para iniciar sesión en el ordenador y en otros dispositivos, incluido el propio dispositivo móvil. En la verificación en dos pasos pueden utilizarse tokens de software y hardware basados en el estándar TOTP (contraseña temporal de un solo uso).
- Códigos de seguridad: Si un usuario no tiene acceso a su dispositivo móvil o trabaja en una zona en la que no puede llevarlo, puede utilizar códigos de seguridad como parte de la verificación en dos pasos. Para ello, solo tiene que generar un código de verificación de reserva e imprimirlo con antelación.
- Mensaje de texto o llamada telefónica: Google envía un código de verificación en dos pasos a dispositivos móviles a través de un mensaje de texto o una llamada.

El propio fabricante recomienda utilizar las llaves de seguridad, ya que son el método de verificación en dos pasos más seguro. Otra opción es que los usuarios utilicen la llave de

seguridad integrada de su teléfono (disponible en teléfonos con Android 7 y versiones posteriores o iOS 10 y versiones posteriores).

Alternativas a las llaves de seguridad en caso de decidir no utilizarlas:
Las mejores alternativas son los mensajes de Google o la aplicación Google Authenticator. Google Authenticator es una aplicación basada en autenticación con contraseña de un solo uso (OTP) desarrollado por Google. Google Authenticator ofrece un número de seis dígitos que el usuario debe proporcionar además de su nombre de usuario y contraseña para acceder a los servicios de Google.

- No se deberá usar los mensajes de texto: este método de verificación en dos pasos depende de redes de operadores de telefonía externos, por lo que se pueden interceptar.

### 2.1.2 Explotación

#### 2.1.2.1 Inventario de activos

Este apartado del marco operacional del Esquema Nacional de Seguridad exige el mantenimiento de un inventario actualizado de activos, incluyendo detalles de naturaleza y responsabilidad.

El usuario de GW deberá apoyarse en los medios de la plataforma para cumplir con este requisito que se detallarán a continuación.

Dentro de GW, las cuentas de administradores tienen acceso a los informes de la consola de administración de Google, donde se pueden examinar posibles riesgos de seguridad, medir la colaboración de los usuarios, controlar quién inicia sesión y cuándo lo hace, o analizar la actividad de los administradores. Estos informes permiten consultar tanto datos generales de todo el dominio como información detallada sobre usuarios concretos.

*figura 4. Vista de la consola de administración con los paneles de elementos compartidos a usuarios externos y número de autenticaciones dentro del dominio de la organización.*

Los tipos de informes que podemos obtener de la consola son los siguientes:

- Informe Destacado: En este informe se puede ver el uso que hace un equipo de los servicios de Google Workspace, la visibilidad de los documentos de Drive, el espacio de almacenamiento, el uso compartido de archivos y métricas de seguridad básicas.
- Informes de aplicaciones de toda la organización: Permite consultar información administrativa.
- Informe de usuario - Cuentas: Muestra la información más destacada de seguridad y del uso de las aplicaciones.
- Informe de usuario - Uso de aplicaciones: Muestra la información sobre el uso de aplicaciones como Drive y Gmail.
- Informe de usuario - Seguridad: Evalúa el riesgo al que están expuestos los datos del dominio y permite obtener información de las aplicaciones de terceros instaladas en los dispositivos móviles o los documentos compartidos fuera del dominio.
- Registros de auditoría: Permite obtener eventos concretos como las actividades de los administradores o de los diferentes usuarios y dispositivos.
- Se deberá mantener un inventario actualizado de todos los elementos del sistema, detallando su naturaleza e identificando a su responsable; es decir, la persona que es responsable de las decisiones relativas al mismo.

#### 2.1.2.2 Protección frente a código dañino

Google Workspace ofrece una herramienta que ayuda a proteger las cuentas registradas dentro del dominio. Esta herramienta es el Programa de Protección Avanzada.


*figura 5. Pantalla de registro al Programa de Protección Avanzada.*

El Programa de Protección Avanzada está diseñado para proteger las cuentas de Google frente a ataques malintencionados online. Los ataques mal intencionados pueden ser ataques de phishing a pequeña escala que a menudo van dirigidos contra individuos concretos, y puede ser difícil distinguirlos de las actividades legítimas. Por este motivo, son los ataques más difíciles de controlar.

Para habilitar el programa de Protección Avanzada, se adjunta la guía del fabricante: https://support.google.com/a/answer/9378768?hl=es&ref_topic=9376233

Este programa de Protección Avanzada incluye un conjunto de políticas de alta seguridad seleccionadas que se aplican a las cuentas registradas. La Protección Avanzada te permite aplicar todas estas protecciones a la vez y anular ajustes similares que se hayan configurado manualmente. Estas políticas incluyen:

- Autenticación segura con llaves de seguridad: Con el Programa de Protección Avanzada se exige el uso de llaves de seguridad para el inicio de sesión. El uso de la llave de seguridad se aplica incluso si un dominio utiliza un proveedor de identidades (IdP) externo.
- Uso de códigos de seguridad con llaves de seguridad (según sea necesario): El uso de códigos de seguridad con llaves de seguridad reduce la protección. Sin embargo, es posible que haya procesos importantes en los que las llaves de seguridad no se puedan utilizar directamente y, en ese caso, se requieran códigos de seguridad.

- Restricciones sobre el acceso de terceros a los datos de la cuenta: Las aplicaciones que requieren acceso a datos de alto riesgo se bloquean a menos que los administradores confíen en ellas de forma explícita o que aparezcan en la lista predeterminada de aplicaciones de confianza.
- Análisis exhaustivos de Gmail: Los análisis mejorados de mensajes antes de su entrega se habilitan automáticamente para identificar los intentos de phishing. La función de zona de pruebas de seguridad está activada para proporcionar un análisis profundo de los archivos adjuntos en busca de software malicioso desconocido.
- Protecciones de Navegación Segura de Google en Chrome: Reduce el riesgo de que los usuarios descarguen archivos peligrosos en Google Chrome.
- Recuperación de la cuenta por medio del administrador: Recuperación rigurosa de cuentas para que, cuando los usuarios pierdan sus llaves de seguridad, recurran al administrador para volver a acceder a su cuenta.

Puede obtener más información sobre su implementación en la siguiente guía del fabricante:
https://support.google.com/a/answer/9378686?hl=es

- Se deberá habilitar el registro de usuarios en el Programa de Protección Avanzada.

Cuando un usuario se registra, las políticas que se hayan configurado manualmente quedan anuladas por las del programa de Protección Avanzada. Por ejemplo, si no se ha aplicado la verificación en dos pasos en la organización y algunos usuarios se registran en Protección Avanzada, la política de verificación en dos pasos incluida en este programa obliga a configurarla al usuario registrado.

#### 2.1.2.2 Gestión de incidentes

Dentro de GW se encuentra un apartado de alertas por correo electrónico, donde los administradores de la organización reciben un correo cuando un evento importante ocurre dentro del dominio, por ejemplo, cuando se produce un intento de inicio de sesión sospechoso. Estas alertas también son visibles desde la consola de administración de GW.

Estos correos electrónicos de alertas se basan en reglas definidas por el sistema que se pueden encontrar en la página de reglas de seguridad, aunque también se pueden crear alertas personalizadas basadas en los registros de auditoria de la organización. Estas reglas vienen ya definidas por el propio servicio de Google. También se podrán definir nuevas reglas dentro de la consola de administración de Google. Además, también podemos definir qué acciones debe tomar el sistema en caso de saltar una de estas reglas.

Hay diferentes tipos de reglas que se pueden crear:

- Reglas de actividad: son reglas personalizadas que los administradores de dominio crean a partir de los datos de la herramienta de investigación de seguridad o desde la página de reglas. Con estas reglas, se pueden automatizar acciones para que se realicen en respuesta a actividades que tienen lugar en el dominio.
- Reglas de protección de datos: son reglas personalizadas que los administradores de dominio pueden crear desde la página de reglas. Sirven para recibir notificaciones cuando ocurran actividades concretas relacionadas con el uso de archivos de Drive en tu dominio.
- Reglas de informes: permite crear alertas personalizadas basadas en los registros de auditoría de la organización.
- Se deberán mantener las reglas definidas por el sistema activadas y configurar las notificaciones por correo electrónico.

Para la implementación de las reglas de actividad se adjunta la documentación del fabricante:
https://support.google.com/a/answer/9420866#zippy=%2Ccrear-reglas-de-actividad

- Se deberán configurar reglas de actividad y de protección de los datos, que permitan automatizar las acciones que se llevan a cabo en respuesta de las actividades que se producen dentro del dominio de la organización

Para la implementación de las reglas de protección de datos se adjunta la documentación del fabricante:
https://support.google.com/a/answer/9420866#zippy=%2Ccrear-reglas-de-protecci%C3%B3n-de-datos

- Se deberán crear alertas personalizadas basadas en los registros de auditoría de la organización.

Para la implementación de las reglas de informes de datos se adjunta la documentación del fabricante:
https://support.google.com/a/answer/9420866#zippy=%2Ccrear-reglas-de-informes

#### 2.1.2.2 Registro de la actividad de los usuarios

La categoría ALTA del ENS exige el registro de actividades de los usuarios del sistema. Esto incluye usuarios como administradores. Deberán registrarse las actividades realizadas con éxito y los intentos fracasados, así como quien la realiza y sobre qué información.

Los administradores de la organización de GW tendrán acceso a los siguientes informes de usuario además de a los logs de eventos de la actividad realizada por los usuarios, teniendo la opción de filtrar y crear alertas.

**Informes de usuario: cuentas**

Este informe proporciona información relacionada con el estado de las cuentas de usuario y el nivel de seguridad de las contraseñas de las mismas.

Para la generación del informe puede seguir la guía del fabricante:
https://support.google.com/a/answer/4580176?hl=es

Dentro de este informe podemos encontrar los siguientes datos relevantes:

| Columna del informe - General | Descripción |
|---|---|
| Usuario | Nombre de usuario |
| Estado de la cuenta del usuario | El estado de la cuenta del usuario (Activas, Bloqueadas o Suspendidas).<br>• Los usuarios **bloqueados** han infringido los Términos del Servicio.<br>• Los usuarios **suspendidos** tienen una cuenta que ha sido inhabilitada temporalmente por un administrador.<br>El estado de la cuenta del usuario **Activas** incluye los usuarios eliminados de forma no definitiva. |
| Estado del administrador | El acceso de administrador de un usuario: Superadministrador, Administrador o Ninguno. |
| Inscripción en la verificación en dos pasos | Indica si el usuario está registrado en la verificación en dos pasos. |
| Implementación obligatoria de la verificación en dos pasos | Indica si el usuario debe estar registrado en la verificación en dos pasos. |
| Conformidad con la política de longitud de la contraseña | Indica si el usuario cumple o no los requisitos de longitud de la contraseña. |
| Nivel de seguridad de la contraseña | Indica si el usuario tiene una contraseña segura o poco segura según los requisitos de las contraseñas definidos por un administrador. |
| Aplicaciones externas | El número de aplicaciones externas (que no son de Google) que el usuario ha instalado en tu dominio. |

| Columna del informe - General | Descripción |
|---|---|
| Acceso a aplicaciones poco seguras | Indica si el usuario tiene la opción de bloquear o permitir (Permitido o Rechazado ) el acceso de las aplicaciones poco seguras a sus propias cuentas. |
| Nombre definido por el administrador | El nombre de usuario designado por el administrador. |
| Estado del nombre de perfil | Indica si el usuario ha cambiado el nombre de su perfil o no lo ha modificado. |

| Columna del informe - Gmail | Descripción |
|---|---|
| Total de correos electrónicos | El número de mensajes de Gmail que el usuario ha enviado y recibido. Se incluyen los correos electrónicos enviados o recibidos de clientes SMTP de terceros que usan servidores SMTP de Gmail. |
| Correos electrónicos recibidos | El número de mensajes de Gmail que el usuario ha recibido. Se incluyen los correos electrónicos recibidos de clientes SMTP de terceros que usan servidores SMTP de Gmail. |
| Correos electrónicos enviados | El número total de mensajes de Gmail que el usuario ha enviado. Se incluyen los correos electrónicos enviados por clientes SMTP de terceros que usan servidores SMTP de Gmail. |
| Gmail (POP): usado por última vez | La última vez que el usuario usó un servidor de correo con el protocolo de oficina postal (POP) para acceder a Gmail. |
| Gmail (IMAP): usado por última vez | La última vez que el usuario usó un servidor de correo con el protocolo de acceso a mensajes de Internet (IMAP) para acceder a Gmail. |
| Gmail (Web): usado por última vez | La última vez que el usuario usó la versión web de Gmail. |

| Columna del informe - Drive | Descripción |
|---|---|
| Público | El número de archivos disponibles públicamente. |
| Cualquier usuario con el enlace | El número de archivos de Drive disponibles para todos los usuarios que dispongan del enlace. |
| Archivos compartidos con cualquier usuario del dominio | El número de archivos de Drive que se comparten con todos los usuarios del dominio. |
| Archivos compartidos con cualquier usuario del dominio que tenga el enlace | El número de archivos de Drive disponibles para todos los usuarios del dominio que dispongan del enlace. |
| Fuera del dominio | El número de archivos de Drive que se han compartido expresamente con usuarios o grupos de fuera del dominio. |
| Archivos compartidos en el dominio | El número de archivos de Drive que se han compartido expresamente con usuarios o grupos del dominio. |
| Archivos compartidos de forma privada | El número de archivos de Drive que no se comparten. |
| Otros tipos añadidos | El número de archivos que no son de Google que ha añadido el usuario. |
| Archivos editados | El número de archivos de Drive que ha editado el usuario. |
| Archivos vistos | El número de archivos de Drive que ha visto el usuario. |
| Archivos añadidos | El número de archivos de Drive que ha añadido el usuario. |
| Drive: último momento de actividad | La última vez que el usuario utilizó Drive. |
| Público | El número de archivos disponibles públicamente. |

**Nota**: Algunos campos se han omitido porque no son relevantes.

**Informes de usuario: seguridad**

Este informe proporciona un resumen completo de cómo comparten datos los usuarios, cómo acceden a ellos y si toman las precauciones de seguridad necesarias. En él se puede consultar, por ejemplo, quiénes instalan aplicaciones externas, comparten muchos archivos, se saltan la verificación en dos pasos o usan llaves de seguridad.

Para la generación del informe puede seguir la guía del fabricante:
https://support.google.com/a/answer/6000269?hl=es&ref_topic=9026833

Dentro de este informe podemos encontrar los siguientes datos relevantes:

| Columna del informe - General | Descripción |
|---|---|
| Aplicaciones externas | El número de aplicaciones de terceros con autorización para acceder a los datos de un usuario. |
| Registro en la verificación en dos pasos | Indica si un usuario se ha registrado en la verificación en dos pasos. |
| Implementación obligatoria de la verificación en dos pasos | Indica si un usuario está obligado a registrarse en la verificación en dos pasos. |
| Conformidad con la política de longitud de la contraseña | Indica si el usuario cumple o no los requisitos de longitud de la contraseña. |
| Nivel de seguridad de la contraseña | Indica si el usuario tiene una contraseña segura o poco segura según los requisitos de las contraseñas definidos por un administrador. |
| Estado de la cuenta del usuario | El estado de la cuenta del usuario (Activas, Bloqueadas o Suspendidas). |
| Estado del administrador | El acceso de administrador de un usuario: Superadministrador, Administrador o Ninguno. |
| Acceso a aplicaciones poco seguras | Indica si el usuario puede bloquear o permitir el acceso de las aplicaciones poco seguras a sus propias cuentas (Denegado o Permitido, respectivamente). |
| Llaves de seguridad registradas | El número total de llaves de seguridad registradas por los usuarios de este dominio. |

| Columna del informe - General | Descripción |
|---|---|
| Aplicaciones externas | El número de aplicaciones de terceros con autorización para acceder a los datos de un usuario. |
| Registro en la verificación en dos pasos | Indica si un usuario se ha registrado en la verificación en dos pasos. |

| Columna del informe - Drive | Descripción |
|---|---|
| Archivos compartidos con usuarios externos | El número de eventos que se registran cuando el usuario comparte archivos con usuarios externos. |
| Archivos compartidos con usuarios internos | El número de eventos que se registran cuando el usuario comparte archivos con usuarios internos. |
| Público | El número de eventos que se registran cuando el usuario del dominio comparte archivos que están disponibles públicamente. |
| Cualquier usuario con el enlace | El número de eventos que se registran cuando el usuario del dominio comparte archivos que están disponibles para todos los usuarios que dispongan del enlace. |
| Archivos compartidos con cualquier usuario del dominio que tenga el enlace | El número de eventos que se registran cuando el usuario del dominio comparte archivos que están disponibles para todos los usuarios del dominio que dispongan del enlace. |
| Archivos compartidos con cualquier usuario del dominio | El número de eventos que se registran cuando el usuario del dominio comparte archivos que pueden ver todos los usuarios del dominio. |
| Fuera del dominio | El número de eventos que se registran cuando el usuario del dominio comparte archivos explícitamente con personas o grupos que están fuera del dominio. |

| Columna del informe - Drive | Descripción |
|---|---|
| Archivos compartidos en el dominio | El número de eventos que se registran cuando el usuario del dominio comparte archivos explícitamente con personas o grupos del dominio. |
| Archivos compartidos de forma privada | El número de archivos de Drive que no se comparten. |

**Informes de usuarios: uso de las aplicaciones**

Este informe proporciona información relacionada con la actividad de los usuarios, como los correos enviados durante un periodo específico, la cantidad de archivos que crean y comparten, cuáles de ellos están a punto de alcanzar los límites de almacenamiento y el número de consultas de búsqueda que se han hecho desde diferentes tipos de dispositivos.

Para la generación del informe puede seguir la guía del fabricante:
https://support.google.com/a/answer/4579578?hl=es&ref_topic=9026833

### 2.1.3 Continuidad del servicio

Google Workspace es un servicio que opera completamente online, por ello es importante tener en cuenta los desastres vinculados con las tecnologías de la información, pérdidas de conexión o interrupción del servicio. GW ofrece una serie de características que nos permite minimizar los riesgos relacionados con la continuidad del servicio.

#### 2.1.3.1 Plan de continuidad

Cuando el servicio de GW sufra alguna caída o un usuario no tenga acceso a Internet, se podrá configurar el uso de Gmail, Calendar y Drive para que pueda ser accesible sin conexión.

**Drive**

El acceso sin conexión está habilitado de forma predeterminada en las organizaciones, así que los usuarios pueden activarlo en sus propias cuentas cuando quieran.

- Para controlar el acceso sin conexión, se deberán usar políticas gestionadas en cada ordenador.

Se tienen que aplicar políticas gestionadas para cada ordenador de manera individual. Con esta opción los usuarios solo podrán activar la opción de sin conexión si se ha instalado primero una política gestionada en su ordenador.

Instalar la política en todos los ordenadores gestionados:
Para permitir que se guarden archivos de Google Drive en ordenadores gestionados y que se acceda a ellos sin conexión, puedes seguir la guía del fabricante:
https://support.google.com/a/answer/1642623?hl=es-419

**Gmail**
El acceso sin conexión con el servicio de Gmail permite poder leer, escribir, buscar, eliminar y etiquetar mensajes de correo electrónico sin necesidad de tener conexión a internet. En el momento que se restablezca el servicio, Gmail actualizará de manera automática.

- Para que los usuarios puedan acceder a Gmail sin conexión, se debe habilitar esta función desde la consola de administración. Además, cada usuario debe habilitar esta función de manera personal.

Puede obtener más información sobre cómo configurar este servicio desde el siguiente documento del fabricante:
https://support.google.com/a/answer/7684186?hl=es

### 2.1.4 Monitorización del sistema

La monitorización del sistema comprende el conjunto de actividades y estará sujeto a medidas de monitorización de la actividad de una entidad, usuario o proceso.

Dentro de GW, los administradores, en el Centro de alertas pueden ver notificaciones sobre posibles problemas en el dominio, así como tomar ciertas medidas para resolverlos (por ejemplo, informar a los usuarios finales o actualizar políticas o ajustes) y, de este modo, proteger la organización frente a amenazas de seguridad.

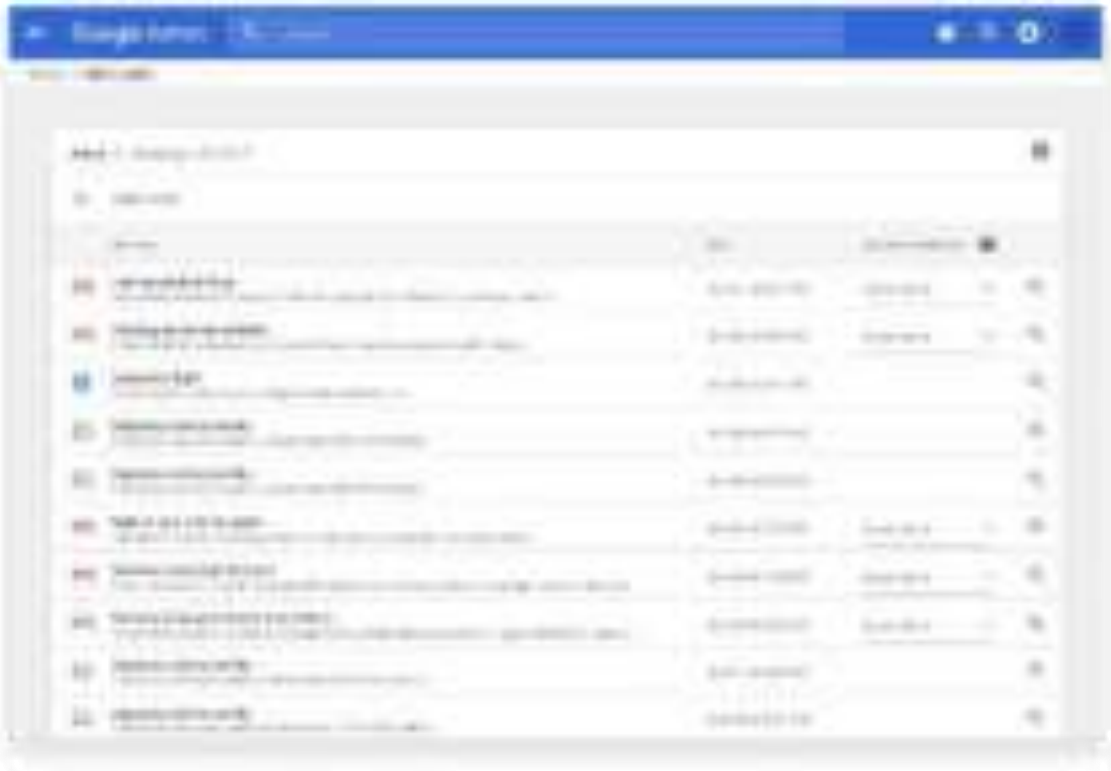

*figura 6. Centro de alertas de Google Workspace*

Se puede crear, editar y ver reglas de informes en la página Informes o en la página Reglas de seguridad. Las reglas de informes se basan en los registros de auditoría de la organización.

Para la implementación, edición o modificación de las reglas y alertas puedes seguir la guía del fabricante:
https://support.google.com/a/answer/9908423?hl=es

#### 2.1.4.1 Detección de intrusión

Dentro de la plataforma de GW, se tiene acceso al panel de seguridad, el cual ofrece una serie de informes que reportan, entre muchas otras métricas, los intentos de inicio de sesión sospechosos o la actividad sospechosa que ha habido en diferentes dispositivos.
**Es importante recalcar que el rango máximo a consultar son 180 días.*

*figura 7. Paneles de información dentro del panel de Seguridad de Google Admin.*

Cuando se consulta el panel de seguridad del dominio de GW, se pueden consultar, entre otros, informes con información relevante a la hora de monitorizar si alguna de las cuentas de nuestra organización está siendo atacada o realizando alguna acción sospechosa. Esta información se puede encontrar en los siguientes informes:

| Informe | Datos disponibles |
|---|---|
| Visibilidad de archivos | En este panel se pueden ver cuántas veces se han compartido archivos con usuarios ajenos al dominio durante un periodo concreto, así como el número de consultas |
| Autenticación | Algunos estándares de autenticación de correo electrónico, como DKIM y SPF, pueden proteger el dominio de determinadas amenazas relacionadas con el correo electrónico, como la suplantación de |

| Informe | Datos disponibles |
|---|---|
| | identidad (phishing). En el gráfico de este panel se muestran los mensajes desglosados según si se han autenticado o no. |
| Configuración personalizada | En el panel Configuración personalizada, se puede ver rápidamente cuántos mensajes de tu dominio no concuerdan con los filtros de spam y la configuración personalizada de Gmail. |
| Incidentes de DLP | Se pueden utilizar reglas de prevención de la pérdida de datos (DLP) para controlar qué información sensible pueden compartir los usuarios.<br><br>En el panel Incidentes de DLP se puede saber cuántos incidentes de este tipo se produjeron. Los incidentes aparecen desglosados en tres niveles de gravedad (alta, media y baja). |
| Incidentes relacionados con las principales políticas | En el panel Incidentes relacionados con las principales políticas, se puede consultar las principales políticas que han causado el mayor número de incidentes.<br><br>En el gráfico se puede ver el número de incidentes relacionados con cada política desglosada por servicio (por ejemplo, Google Drive). |
| Filtro de spam: Todo | En el panel Filtro de spam: Todos, se pueden consultar cuántos mensajes se han marcado como spam, ataques de suplantación de identidad o software malicioso.<br><br>Si un mensaje se considera sospechoso, pero también tiene cualidades positivas (por ejemplo, el remitente está en una lista blanca), es posible que aparezca en la bandeja de entrada del destinatario. |

| Informe | Datos disponibles |
|---|---|
| Filtro de spam: Suplantación de identidad (phishing) | En el panel Filtro de spam: Suplantación de identidad (phishing), se puede consultar cuántos mensajes se han marcado como ataques de suplantación de identidad. |
| Filtro de spam: Software malicioso | En el panel Filtro de spam: Software malicioso, se pueden consultar cuántos mensajes se han identificado como software malicioso.<br><br>Los mensajes entrantes pueden clasificarse como software malicioso antes o después de haberse enviado a la bandeja de entrada de un usuario:<br><br>• Antes de la entrega: los mensajes con archivos adjuntos que se han marcado como software malicioso antes de entregarse se envían a las carpetas de spam de los usuarios con los archivos adjuntos inhabilitados.<br>• Tras la entrega: los mensajes con archivos adjuntos que superan los análisis iniciales de software malicioso se envían a las bandejas de entrada de los usuarios. No obstante, es posible que se identifiquen como software malicioso después de someterlos a un análisis más exhaustivo. Si se clasifican como software malicioso, los archivos adjuntos se inhabilitan. |
| Intentos fallidos de introducir la contraseña en dispositivos | Se considera que se produce un intento fallido de introducir la contraseña cuando se escribe una contraseña incorrecta 6 veces consecutivas en un dispositivo. Cada intento posterior cuenta como un intento fallido más. Por ejemplo, por 6 intentos fallidos consecutivos se contaría 1 intento fallido; por 7 se contarían 2; por 8, 3; y así sucesivamente. |

| Informe | Datos disponibles |
|---|---|
| | En el panel Intentos fallidos de introducir la contraseña en dispositivos, se puede ver cuántas veces se ha intentado introducir una contraseña incorrecta en dispositivos a lo largo del tiempo. |
| Eventos de vulneración de dispositivos | Un dispositivo se considera vulnerado si se detectan en él ciertas actividades sospechosas. Estas actividades varían en función del tipo de dispositivo:<br>• Dispositivos iOS: se considera que un dispositivo iOS se ha vulnerado si se le ha aplicado un jailbreak, ya que en ese caso podrían instalarse en él aplicaciones que no son oficiales, editar ajustes restringidos o saltarse controles de seguridad.<br>• Dispositivos Android: se considera que un dispositivo Android se ha vulnerado si se ha rooteado. Al rootear un dispositivo, los usuarios podrían modificar su código de software e instalar aplicaciones que los fabricantes normalmente no permiten. |
| Actividades sospechosas en dispositivos | Se considera que modificar las propiedades de los dispositivos móviles es una actividad sospechosa. Entre estas propiedades se incluyen el número de serie, el modelo del dispositivo y el nombre del sistema operativo, entre otros datos. |
| Permisos de OAuth concedidos por producto (solo para clientes que usen la versión beta) | Con los permisos de OAuth, las aplicaciones pueden solicitar un acceso limitado y bien definido a determinados datos del usuario. Al especificar permisos de OAuth, una aplicación permite al usuario saber qué permisos o acceso necesita. Estas aplicaciones solo tienen acceso si el usuario en cuestión lo permite. |

| Informe | Datos disponibles |
|---|---|
| | En el panel se pueden ver cuántos permisos de OAuth se han dado a lo largo del tiempo |
| Actividad de autenticación OAuth | OAuth (autorización abierta) es un estándar abierto que concede permiso a servicios de terceros para acceder a la información de la cuenta de un usuario sin mostrar su contraseña.<br><br>Se puede supervisar la actividad de autenticación OAuth de la organización desde el panel Actividad de autenticación OAuth.<br><br>Las aplicaciones del panel Actividad de autenticación OAuth aparecen ordenadas de mayor a menor según el número de cambios que se hayan producido en este tipo de actividad durante un periodo determinado. |
| Autenticaciones OAuth para nuevas aplicaciones | En el panel Autenticaciones OAuth para nuevas aplicaciones, se puede supervisar qué nuevas aplicaciones han recibido tokens de OAuth. |
| Archivos adjuntos sospechosos | En este panel se pueden ver la cantidad de mensajes que incluyen archivos adjuntos sospechosos |
| Spoofing | En el panel Spoofing se puede consultar el número de mensajes en los que hay indicios de posible spoofing. Algunos mensajes que muestran estos indicios pueden suponer un intento de suplantación de identidad (phishing). |

## 2.2 Medidas de protección

### 2.2.1 Protección de la información

#### 2.2.1.1 Calificación de la información

En este punto se determinará como recabar información sobre los archivos existentes en la organización, así como el responsable de cada información y su control de acceso.

Los administradores, pueden restringir el acceso a los archivos de una unidad compartida. También pueden definir las opciones de acceso predeterminadas de las nuevas unidades compartidas. Estas restricciones puedes darse en una unidad organizativa específica o en toda tu organización.

También pueden impedir que los miembros con acceso de administrador modifiquen la configuración de la unidad compartida.

GW ofrece la posibilidad de impedir que los usuarios saquen contenido de la organización mediante ajustes desde la consola de Administración. Para la modificación de este ajuste, puede consultar la guía del fabricante:
https://support.google.com/a/answer/7662202?hl=es#zippy=%2Cimpedir-que-los-usuarios-saquen-contenido-de-la-organizaci%C3%B3n

Para la auditoria de los archivos disponibles, se debe hacer uso del informe de Visibilidad de archivos, disponible en el panel de control de seguridad. Dentro de este informe se pueden obtener los siguientes datos:

- Los diferentes métodos usados para compartir la información.
- Los archivos compartidos que se han visto con más frecuencia
- Los dominios externos con los que se ha compartido un archivo.
- Las reglas de prevención de la pérdida de datos que se han activado con más frecuencia.

Para generar el informe puede consultar la guía del fabricante:
https://support.google.com/a/answer/7491249?hl=es

En la mitad inferior de la página del informe "Visibilidad de archivos", se muestra un gráfico en el que figuran las principales reglas de prevención de la pérdida de datos (DLP) que se han activado en el dominio, así como el número de veces que lo han hecho.

Con las reglas de prevención de pérdida de datos, los administradores pueden evitar que los usuarios compartan contenido sensible con personas ajenas al dominio de la empresa, permitiendo la creación de alertas en caso de que alguna de estas reglas sea incumplida.

Las reglas de DLP activan un análisis de los archivos en busca de contenido sensible e impiden que los usuarios compartan ese contenido. Asimismo, determinan la naturaleza de los incidentes relacionados con DLP, que provocan acciones, como el bloqueo de cierto contenido.

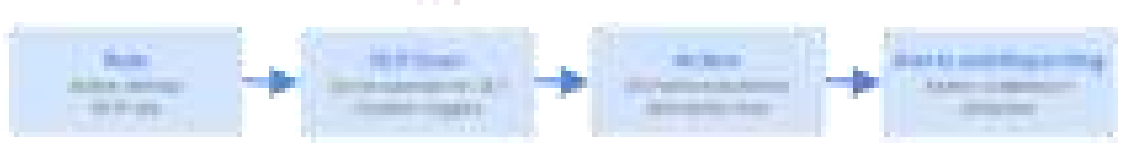

*figura 9. Flujo de DLP.*

Puede consultar más información sobre las reglas DLP en la documentación oficial del fabricante:
https://support.google.com/a/answer/9646351?visit_id=637594651766491617-1928799462&rd=1

#### 2.2.1.2 Limpieza de documentos

**Google Vault**

Vault es una herramienta que permite controlar la información. Con Vault, puedes conservar, bloquear, buscar y exportar los datos de los usuarios de Google Workspace.

Las acciones que se pueden realizar son:

- Conservar datos durante el tiempo que sea necesario. Si tu organización debe conservar datos durante un periodo determinado, puedes configurar Vault para hacerlo. Esos datos estarán disponibles en Vault, aunque los usuarios los borren o vacíen sus papeleras.
- Elimina los datos cuando ya no los necesites. Si tu organización tiene la obligación de eliminar datos sensibles después de cierto tiempo, puedes configurar Vault para que quite esos datos de las cuentas de usuario y los elimine definitivamente de todos los sistemas de Google.

Las reglas de conservación de Vault se aplican directamente a los sistemas de datos de los servicios de Google compatibles. Vault no es un archivo de datos. Una vez que venzan las reglas de conservación, los datos estarán sujetos a los procesos de eliminación estándar. Cuando finaliza el periodo de conservación y se eliminan definitivamente los datos, los usuarios y los administradores no pueden recuperarlos.

Nota: Vault no conserva los datos hasta que configures reglas de conservación. Mientras tanto, los usuarios pueden eliminar sus datos y los servicios pueden eliminarlos de manera definitiva según el protocolo del servicio correspondiente.

Puedes consultar más información sobre este servicio en la web del fabricante:
https://support.google.com/vault/answer/2462365?hl=es

### 2.2.2 Protección de los servicios

#### 2.2.2.1 Protección del correo electrónico

**Asegurar la entrega del correo electrónico**

Para asegurar la entrega segura de los correos electrónicos y proteger la organización frente a correos electrónicos falsificados, deberemos configurar el Sender Policy Framework (SPF). SPF impide que los mensajes del dominio se envíen a las carpetas de spam o correo basura. Si el dominio no utiliza SPF, los servidores de correo que reciben los mensajes no pueden comprobar que los mensajes del dominio sean realmente auténticos.

- Se recomienda además configurar los métodos de autenticación de correo DomainKeys Identified Mail (DKIM) y la política de autenticación basada en dominios para mensajes, informes y conformidad (DMARC).

Para la implementación puede consultar la siguiente guía del fabricante:
https://support.google.com/a/answer/33786?hl=es&ref_topic=10685331#zippy=

Además de lo comentado anteriormente, Google Workspace ofrece la posibilidad de identificar contenido sospechoso. Para ello:

- Se deberá activar el **Análisis mejorado de mensajes antes de la entrega** para identificar con mayor precisión el contenido sospechoso, disponible en la consola de administración.

*figura 10. Activación del Análisis mejorado de mensajes antes de la entrega*

De manera adicional, GW ofrece S/MIME alojado para aumentar la seguridad de los mensajes. Para que funcione el cifrado S/MIME, todos los remitentes y destinatarios deben tenerlo habilitado. Además, deben intercambiar las claves para identificarse de forma única. También se puede evitar enviar o recibir determinados mensajes a menos que estén cifrados o firmados con S/MIME.

## 3. GLOSARIO

A continuación, se describen los términos, acrónimos y abreviaturas relacionados con la tecnología objeto de esta guía con el objeto de facilitar la comprensión de la misma:

| Término | Definición |
|---|---|
| GCDS | Google Cloud Directory Sync. Servicio para sincronizar tus usuarios, grupos y contactos compartidos de Google de forma que coincidan con la información que figura en tu servidor LDAP. |
| GSPS | G Suite Password Sync. Permite sincronizar automáticamente las contraseñas de Google Workspace de tus usuarios con las de Microsoft Active Directory |
| SSO | Single Sign-On. El "Inicio de Sesión Único" es un procedimiento de autenticación que habilita a un usuario determinado para acceder a varios sistemas con una sola instancia de identificación. |
| SPF | Sender Policy Framework. Es una protección contra la falsificación de direcciones en el envío de correo electrónico. Identifica, a través de los registros de nombres de dominio (DNS), a los servidores de correo SMTP autorizados para el transporte de los mensajes. Este convenio busca ayudar a disminuir abusos como el spam y otros. |
| DKIM | Domain Keys Identified Mail. Es una técnica de autenticación de correo electrónico que permite al receptor ver que un correo electrónico fue sin duda, enviado y autorizado por el dueño de ese dominio |
| DMARC | Domain-based Message Authentication, Reporting and Conformance. Es un mecanismo de autenticación de correo electrónico. Ha sido diseñado para otorgar a los propietarios de dominios de correo electrónico la capacidad de proteger su dominio del uso no autorizado, comúnmente conocido como email spoofing. |

# 4. GLOSARIO DE SERVICIOS GW

A continuación, se reúnen los diferentes servicios mencionados a lo largo de esta guía incluyendo enlaces a la documentación concreta de cada uno de ellos.

| Servicio | URL de documentación servicio |
|---|---|
| **Gmail** | https://support.google.com/a/users/answer/9259748?visit_id=637564950795859562-1351620081&hl=es&rd=1 |
| **Drive** | https://support.google.com/drive/?hl=es#topic=14940 |
| **Meet** | https://support.google.com/a/users/answer/9282720?hl=es |
| **Calendar** | https://support.google.com/a/users/answer/9247501?visit_id=637564950795859562-1351620081&hl=es&rd=1 |
| **Chat** | https://support.google.com/a/users/answer/9247502 |
| **Currents** | https://support.google.com/a/users/answer/9247362?visit_id=637564950795859562-1351620081&hl=es&rd=1 |
| **Jamboards** | https://support.google.com/jamboard/?hl=es#topic=7383643 |
| **Docs** | https://support.google.com/a/users/answer/9282664?visit_id=637564950795859562-1351620081&rd=1 |
| **Sheet** | https://support.google.com/a/users/answer/9282959?visit_id=637564950795859562-1351620081&rd=1 |
| **Slides** | https://support.google.com/a/users/answer/9282488?visit_id=637564950795859562-1351620081&rd=1 |
| **Keep** | https://support.google.com/a/users/answer/9991367?visit_id=637564950795859562-1351620081&rd=1 |
| **Sites** | https://support.google.com/a/users/answer/9282722?visit_id=637564950795859562-1351620081&rd=1 |
| **Forms** | https://support.google.com/a/users/answer/9991170 |
| **Vault** | https://support.google.com/vault/answer/2462365?hl=es&ref_topic=2739742 |

## 5. CUADRO RESUMEN DE MEDIDAS DE SEGURIDAD

Se facilita a continuación un cuadro resumen de configuraciones a aplicar para la protección del servicio. Estas medidas sirven para valorar el nivel de cumplimiento de la organización.

| Control ENS | Descripción medida | Identificador control guías ENS GC | Descripción control | Chequeo automatizado |
|---|---|---|---|---|
| [op.acc.1] | Identificación | [op.acc.1.gw.iam.1] | Se deberá aplicar la autenticación multifactor de manera obligatoria. | |
| | | [op.acc.1.gw.iam.2] | Se deberá aplicar la política de contraseñas únicas, es decir, no usar la misma contraseña en cuentas diferentes, ya sean de la misma organización o de servicios externos a la misma. | |
| | | [op.acc.1.gw.iam.3] | Se deberá activar las alertas de actividad en las cuentas para supervisar la actividad de las mismas. | |
| | | [op.acc.1.gw.iam.4] | En caso de sospecha de que se ha vulnerado una cuenta, se deberá revisar los dispositivos asociados a la cuenta y evaluar la exposición de la misma, así como la comprobación de si se ha configurado algún ajuste malicioso. | |
| | | [op.acc.1.gw.iam.5] | Se deberá crear una cuenta de administrador por cada super administrador, cada una de ellas gestionada por una persona diferente. | |
| | | [op.acc.1.gw.iam.6] | Control activo de la consola de administración de Google para ver el historial de las tareas realizadas por cada cuenta de administrador. | |

| Control ENS | Descripción medida | Identificador control guías ENS GC | Descripción control | Chequeo automatizado |
|---|---|---|---|---|
| | | [op.acc.1.gw.iam.7] | Se deberá generar un código de seguridad para que en caso de pérdida de contraseña o de la clave de la doble verificación se permita recuperar la cuenta. Esta clave deberá ser guardada en un lugar seguro. | |
| | | [op.acc.1.gw.iam.8] | Las cuentas de administradores se deberán usar solo para realizar tareas que requieren de un super administrador. | |
| [op.acc.2] | Requisitos de acceso | [op.acc.2.gw.org.1] | Se deberán crear unidades organizativas distintas para usuarios y dispositivos. De esta forma, se podrán personalizar los ajustes de los dispositivos y los usuarios gestionados según sea necesario. | |
| | | [op.acc.2.gw.org.2] | Se deberá revisar el acceso de las aplicaciones de terceros a los servicios principales de Google Workspace y decidir el uso de las mismas. | |
| | | [op.acc.2.gw.org.3] | Se deberá crear una lista de aplicaciones de confianza que incluya las aplicaciones de terceros que puedan acceder a los servicios principales de Google Workspace. | |
| [op.acc.4] | Proceso de gestión de derechos de acceso | [op.acc.4.gw.org.4] | Se deberá usar la menor cantidad de cuentas posible, pero tantas como sea necesario. | |
| | | [op.acc.4.gw.org.5] | Se deberán usar cuentas diferentes para la etapa de pruebas y de producción. Se crearán algunos usuarios para la etapa de pruebas que los administradores puedan usar para verificar los cambios de la configuración. | |

| Control ENS | Descripción medida | Identificador control guías ENS GC | Descripción control | Chequeo automatizado |
|---|---|---|---|---|
| [op.acc.5] | Mecanismo de autenticación | [op.acc.5.gw.iam.9] | No se deberá usar los mensajes de texto: este método de verificación en dos pasos depende de redes de operadores de telefonía externos, por lo que se pueden interceptar. | |
| [op.exp.1] | Inventario de activos | [op.exp.1.gw.inf.1] | Se deberá mantener un inventario actualizado de todos los elementos del sistema, detallando su naturaleza e identificando a su responsable; es decir, la persona que es responsable de las decisiones relativas al mismo. | |
| [op.exp.6] | Protección frente a código dañino | [op.exp.6.gw.conf.1] | Se deberá habilitar el registro de usuarios en el Programa de Protección Avanzada. | |
| [op.exp.7] | Gestión de incidentes | [op.exp.7.gw.conf.2] | Se deberán mantener las reglas definidas por el sistema activadas y configurar las notificaciones por correo electrónico. | |
| | | [op.exp.7.gw.conf.3] | Se deberán configurar reglas de actividad que permitan automatizar las acciones que se llevan a cabo en respuesta de las actividades que se producen dentro del dominio de la organización | |
| | | [op.exp.7.gw.conf.4] | Se deberán crear alertas personalizadas basadas en los registros de auditoría de la organización. | |
| [op.cont.2] | Plan de continuidad | [op.cont.2.gw.conf.5] | Para controlar el acceso sin conexión, se deberán usar políticas de control de acceso. | |

| Control ENS | Descripción medida | Identificador control guías ENS GC | Descripción control | Chequeo automatizado |
|---|---|---|---|---|
| | | [op.cont.2.gw.conf.6] | Para que los usuarios puedan acceder a Gmail sin conexión, se debe habilitar esta función desde la consola de administración. Además, cada usuario debe habilitar esta función de manera personal. | |
| [mp.s.1] | Protección del correo electrónico | [mp.s.1.conf.7] | Se deberá activar el Análisis mejorado de mensajes antes de la entrega para identificar con mayor precisión el contenido sospechoso, disponible en la consola de administración. | |