PLAN DE TRATAMIENTOS DE RIESGOS SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL 2026

Sistema de Gestión de Seguridad de la Información
Secretaría de Educación Del Distrito

ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA DE EDUCACIÓN
BOGOTÁ

Vigencia 2026

Tabla de Contenido

Índice de Tablas

GLOSARIO

ACTIVOS: en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

ACTIVO DE INFORMACIÓN: bien de la entidad (representado en su información y datos) que tiene valor para los procesos de negocio, independientemente de su ubicación; puede ser un documento físico debidamente firmado, un archivo guardado en un servidor, un aplicativo o cualquier elemento que permita almacenar información valiosa o útil.

AMENAZAS: causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

ANÁLISIS DE RIESGOS: uso sistemático de una metodología para estimar los riesgos e identificar sus fuentes, para los activos o bienes de información.

APETITO DE RIESGO: Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar**.**

CAUSA: Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

CAUSA INMEDIATA: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

CAUSA RAÍZ: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

CONSECUENCIA: los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

Control: Medida que permite reducir o mitigar un riesgo

DISPONIBILIDAD: la disponibilidad consiste en asegurarse que los usuarios autorizados tengan acceso a la información y a los sistemas de apoyo, cuando se requiera, se trata de la propiedad de ser accesible y utilizable, bajo solicitud por una entidad autorizada.

CONTINUIDAD: la continuidad es el proceso de establecer por adelantado, las capacidades necesarias para evitar o mitigar el impacto de un acontecimiento que provoca la interrupción de las operaciones en una o más procesos.

CONFIDENCIALIDAD: propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

CONTROL: es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas, y que pueden ser de carácter administrativo, técnico o legal.

CONTROL DE ACCESO: una característica o técnica en un sistema de comunicaciones para permitir o negar el uso de algunos componentes o algunas de sus funciones.

CRITICIDAD: medida del impacto que tendría la organización debido a una falla de un sistema y que éste no funcione como es requerido.

DISPONIBILIDAD: propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

IMPACTO: el coste para la empresa de un incidente (de la escala que sea), que puede o no ser medido en términos estrictamente financieros.

ISO/IEC 27001:2022: norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa.

MEDIOS DE ALMACENAMIENTO DIGITAL: son todos aquellos dispositivos autorizados por la Secretaría de Educación del Distrito, que permiten el almacenamiento de información, los cuales pueden ingresar o salir de las instalaciones de la entidad con la respectiva autorización. Se incluyen equipos portátiles, teléfonos inteligentes, Ipods, reproductores mp3, memorias USB/SD/Mini-SD, CDs, DVDs, cintas: respaldo y similares. Asimismo, se incluyen correos electrónicos y conexiones por donde pueda ser transportada la información de la Entidad.

MEDIO REMOVIBLE: medio que permite llevar o transportar información desde un computador a otro. Los medios removibles incluyen cintas, diskettes, discos duros removibles, CDs, DVDs, unidades de almacenamiento USB.

PROCEDIMIENTO: los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la organización, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos

procedimentales o técnicos establecidos dentro de la dependencia donde ellos se aplican.

RIESGO: efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de lo esperado: positivo o negativo.

SENSIBILIDAD: nivel de impacto que una divulgación no autorizada podría generar.

SERVICIO: es cualquier acto o desempeño que una persona puede ofrecer a otra, que es esencialmente intangible y que no conlleva ninguna propiedad. Su producción puede o no estar ligada a un producto físico.

TOLERANCIA DEL RIESGO: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.

1. JUSTIFICACIÓN

La Secretaría de Educación del Distrito es una entidad que se encarga de dirigir, organizar y planificar el servicio educativo de conformidad con las disposiciones constitucionales, legales y los fines de la educación establecidos en las leyes que regulan el servicio público educativo, en condiciones de calidad, pertinencia, equidad, eficiencia, y efectividad.

La información que se maneja es de carácter confidencial y amparado por la ley 1098 del 2006, la cual en sus artículos tiene por finalidad “garantizar a los niños, a las niñas y a los adolescentes su pleno y armonioso desarrollo para que crezcan en el seno de la familia y de la comunidad, en un ambiente de felicidad, amor y comprensión. Prevaleciendo el reconocimiento a la igualdad y la dignidad humana, sin discriminación alguna”.

En el marco del Modelo de Seguridad y Privacidad de la Información y el Sistema deGestión de Seguridad de la Información de la SED, el cual busca prevenir los efectos no deseados que se puedan presentar en cuanto a seguridad de la información, la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC a través de su plan de acción 2026, ha establecido como meta el tratamiento de los riesgos de seguridad de la información aplicado a los procesos corporativos, para ello sea apoyado en la Guía para la administración del riesgo y el diseño de controles en entidades públicas Vr. 5[1].

En la vigencia 2025, se definió la metodología para el tratamiento de riesgos de seguridad y privacidad de la información de la SED, de acuerdo con los nuevos lineamientos para la gestión del riesgo de seguridad digital en

[1] https://gobiernodigital.mintic.gov.co/692/articles-82062_recurso_1.pdf

entidades públicas, dispuesto por el Departamento Administrativo de la Función Pública.

2. METODOLOGIA

La metodología empleada para el análisis de riesgo es la aprobada por la SED mediante el documento Metodología de Administración para la gestión de los Riesgos de Seguridad Digital con fecha de resolución 001 del 31/03/2025, la cual se basa en la GUÍA PARA LA GESTIÓN INTEGRAL DEL RIESGO EN ENTIDADES PÚBLICAS V7, entregada por la Alta consejería de las TIC en agosto de 2025, partiendo de los lineamientos del Ministerio de Tecnologías de la Información y Comunicaciones (MINTIC), como líder de la política de gobierno digital, mediante la definición de los lineamientos y metodologías aplicables para la gestión de riesgos de seguridad de la información, que permita incrementar la confianza de las partes interesadas en el uso del entorno digital y del aseguramiento de los activos de información en las entidades.”.

3. OBJETIVO

Mejorar la comprensión de la organización y ampliado su visión sobre su perfil y apetito de riesgo, aclarar el pensamiento sobre la naturaleza y el impacto de los riesgos, y mejorar el modelo de evaluación de riesgos de la SED.

4. ALCANCE

El plan de manejo de riesgos de seguridad digital contempla los procesos del mapa de procesos de la SED, en concordancia con el alcance del Modelo de Seguridad y Privacidad de la Información, habilitador transversal de la Política de Gobierno Digital expedida por el MINTIC.

5. PLAN DE GESTION DE RIESGOS DE SEGURIDAD DIGITAL Y SEGURIDAD DE LA INFORMACIÓN

La Secretaría de Educación del Distrito establece el Plan de Gestión de Riesgos de Seguridad Digital mediante el cual se identifican las amenazas, las vulnerabilidades de seguridad digital y seguridad de la información, el impacto y el nivel de riesgo asociados a los procesos de la entidad, con relación a la valoración de sus activos de información para determinar el tratamiento de sus riesgos según nivel de criticidad establecido.

5.1. Valoración de riesgos

Durante la valoración inicial de activos, con la asesoría de la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC se describe el riesgo de forma cualitativa y/o cuantitativa, se determina el nivel de exposición de los riesgos de seguridad de la información, e identifican las causas de los riesgos que existen (o que podrían existir), se identifica el impacto que podría generar la materialización de cada riesgo, las consecuencias potenciales, y finalmente se priorizan para identificar o proponer el tratamiento de riesgos y su clasificación según los criterios de evaluación determinados por la entidad.

La OTIC recopila y consolida esta información en la matriz de Gestión de Riesgos de Seguridad Digital y de seguridad de la Información.

A continuación, se describe el detalle de las fases que comprende realizar una adecuada valoración de riesgos:

5.2. Identificación de riesgos inherentes

Como lo indica la Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas[2] emitida por el DAFP, para efectos del presente modelo se podrá identificar los siguientes tres (3) riesgos inherentes de seguridad digital:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Para cada riesgo, se deben asociar el grupo de activos de la entidad o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

Una vez establecidos y valorados los riesgos inherentes se procede a la identificación y evaluación de los controles existentes para evitar trabajo o costos innecesarios. Estos controles deben tomar como base el Anexo A de la Norma ISO/IEC 27001:2022.

5.3. Identificación de Amenazas

Se plantean los siguientes listados de amenazas, que representan situaciones o fuentes que pueden hacer daño a los activos y materializar los riesgos.

- **N (**Desastres naturales)

[2] https://www.funcionpublica.gov.co/documents/28587410/38054865/2021-01-20_Guia_administracion_riesgos_f.pdf/6351b4f1-2299-8b6e-70b7-f99f6dd4c59a?t=1611257075079

- **I** (De origen Industrial)
- **EI** (Errores y Fallos no Intencionados).
- **AI** (Ataques Intencionados).
- **NI** (Desastres Naturales e Industriales).

Este análisis arroja como resultado la tabla definición de amenazas, en la cual se han clasificado las amenazas que podrían emplear las vulnerabilidades ya conocidas, que afectan el funcionamiento o disponibilidad de los activos de información.

En este cuadro, se realiza la descripción de las amenazas identificadas, a través de los siguientes ID, los cuales se han definido en la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II - Catálogo de Elementos de Margerit versión 3.0.

Tabla 1 Definición de amenazas

Tipo de Amenaza	ID	Amenaza	Descripción
Desastres naturales (Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.)	N01	Fuego	Incendios: posibilidad de que el fuego acabe con recursos del sistema.
	N02	Daños por agua	inundaciones: posibilidad de que el agua acabe con recursos del sistema.
	N04	Pandemia	Incidentes que pueden ser causados por afectaciones de índole médico y que afectan la disponibilidad del personal y prestación de servicios.
	N*	Desastres naturales	Otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, ... Se excluyen desastres específicos tales como incendios (ver [N.1]) e inundaciones (ver [N.2]). Se excluye al personal por cuanto se ha previsto una amenaza específica [E.31] para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas.
De origen industrial (Sucesos que pueden ocurrir de	I01	Fuego	Incendios: posibilidad de que el fuego acabe con recursos del sistema.
	I02	Daños por agua	Inundaciones: posibilidad de que el agua acabe con recursos del sistema.
	I*	Desastres industriales	Otros desastres debidos a la actividad humana: explosiones, derrumbes, contaminación química, sobrecarga eléctrica, fluctuaciones eléctricas, accidentes de tráfico, Se excluyen amenazas específicas como incendio (ver [I.1]) e inundación (ver [I.2]). Se excluye al personal por cuanto se ha previsto una amenaza específica, [E.18], para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas.
	I03	Contaminación mecánica	Vibraciones, polvo, suciedad.
	I04	Contaminación electromagnética	Interferencias de radio, campos magnéticos, luz ultravioleta.
	I05	Avería de origen físico o lógico	Fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema. En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.

Tipo de Amenaza	ID	Amenaza	Descripción
forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.)	I06	Corte del suministro eléctrico	Cese de la alimentación de potencia
	I07	Condiciones inadecuadas de temperatura o humedad	Deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad.
	I08	Fallo de servicios de comunicaciones	Cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente.
	I09	Interrupción de otros servicios esenciales	Otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, tener, refrigerante.
	I10	Degradación de los soportes de almacenamiento de la información	Como consecuencia del paso del tiempo
	I11	Emanaciones electromagnéticas	Hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque. Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información. Esta amenaza se denomina, incorrecta pero frecuentemente, ataque TEMPEST (del inglés "Transiten Electromagnética Pulse Standard").
Errores y fallos no intencionados (Fallos no intencionales causados por las personas. La numeración no es consecutiva, sino	E01	Errores de los usuarios	Equivocaciones de las personas cuando usan los servicios, datos, etc.
	E02	Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación
	E03	Errores de monitorización (log)	Inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos.
	E04	Errores de configuración	Introducción de datos de configuración erróneos. Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.
	E05	Deficiencias en la organización	Cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión. Acciones descoordinadas, errores por omisión, incumplimientos contractuales, etc.
	E06	Difusión de software dañino	Propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.
	E07	Errores de [re-]encaminamiento	Envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando la información en manos de quien no se espera.
	E08	Escapes de información	La información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.

Tipo de Amenaza	ID	Amenaza	Descripción
que está alineada con los ataques deliberados, muchas veces de naturaleza similar a los errores no intencionados, difiriendo únicamente en el propósito del sujeto.)	E09	Alteración accidental de la información	Alteración accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.
	E10	Destrucción de información (accidental)	Pérdida accidental de información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.
	E11	Vulnerabilidades de los programas (software)	Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario, pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.
	E12	Errores de mantenimiento, actualización de programas (software)	Defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.
	E13	Errores de mantenimiento, actualización de equipos (hardware)	Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.
	E14	Caída del sistema por agotamiento de recursos	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
	E15	Pérdida de equipos	La pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. Se puede perder todo tipo de equipamiento, siendo la pérdida de equipos y soportes de información los más habituales. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.
	E16	Falta de concientización del personal	Un manejo inconsciente de seguridad de la información causara riesgos en el manejo y administración de los activos de información.
	E17	Incumplimiento en la disponibilidad del personal	Ausencia de personal adecuado para el cumplimiento de actividades y funciones específicas y acordes a las necesidades del negocio.
Ataques intencionados	A01	Manipulación de los registros de actividad (log)	Manipulación de los registros de actividad (log)
	A02	Manipulación de la configuración	Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.
	A03	Suplantación de la identidad del usuario	Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente.
	A04	Abuso de privilegios de acceso	Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.
	A05	Uso no previsto	Utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.
	A06	Difusión de software dañino	Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.

Tipo de Amenaza	ID	Amenaza	Descripción
(Fallos deliberados causados por las personas. La numeración no es consecutiva para coordinarla con los errores no intencionados, muchas veces de naturaleza similar a los ataques deliberados, difiriendo únicamente en el propósito del sujeto.)	A07	[Re-]encaminamiento de mensajes	Envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Un atacante puede forzar un mensaje para circular a través de un nodo determinado de la red donde puede ser interceptado. Es particularmente destacable el caso de que el ataque de encaminamiento lleve a una entrega fraudulenta, acabando la información en manos de quien no debe.
	A08	Acceso no autorizado	El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.
	A09	Análisis de tráfico	El atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios. A veces se denomina “monitorización de tráfico”.
	A10	Repudio	Negación a posteriori de actuaciones o compromisos adquiridos en el pasado. Repudio de origen: negación de ser el remitente u origen de un mensaje o comunicación. Repudio de recepción: negación de haber recibido un mensaje o comunicación. Repudio de entrega: negación de haber recibido un mensaje para su entrega a otro.
	A11	Interceptación de información (escucha)	El atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada.
	A12	Modificación deliberada de la información	Alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.
	A13	Destrucción de información (Intencional)	Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.
	A14	Divulgación de información	Revelación de información.
	A15	Manipulación de programas	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.
	A16	Manipulación de los equipos	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.
	A17	Denegación de servicio	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
	A18	Robo	La sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales. El robo puede realizarlo personal interno, personas ajenas a la Organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.
	A19	Ataque destructivo	Vandalismo, terrorismo, acción militar, Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal.

Tipo de Amenaza	ID	Amenaza	Descripción
	A20	Ocupación enemiga	Acceso, control o uso no autorizado de instalaciones, sistemas o activos de información por parte de terceros, comprometiendo su disponibilidad, integridad o confidencialidad.
	A21	Extorsión	Amenaza de causar daño, divulgar información o interrumpir servicios con el fin de obtener beneficios económicos o acceso indebido a recursos de la organización.
	A22	Ingeniería social (picaresca)	Ingeniería social (picaresca): Manipulación de personas mediante engaño o suplantación para obtener información sensible, credenciales o acceso a sistemas sin autorización.

5.4. Identificación de Activos de información

Para el proceso de levantamiento de los activos de información, relacionados con el proceso de Gestión de Tecnologías de Información y Comunicaciones, se ha tomado el inventario de sistemas de información de la entidad, que se detallan en el cuadro Ver Anexo N°2 Activos de Información.

5.5. Determinar la criticidad del activo

Se realiza la valoración de los activos de información del proceso Gestión de Tecnologías de Información y Comunicaciones, lo cual permitirá evaluar el nivel de protección que debe tener cada activo, para ello es necesario dar un valor dependiendo del nivel de importancia para la organización.

Esta clasificación se realizará bajo los criterios de confidencialidad, integridad y disponibilidad, definidos en el cuadro criterios de clasificación de activos.

Tabla 2 Criterios de clasificación de activos

Valor	Nivel	Confidencialidad	Integridad	Disponibilidad
1	BAJA	El acceso no autorizado al activo de información y a la información que este gestiona impacta negativamente de manera leve al proceso evaluado.	La pérdida de la exactitud y el estado completo del activo de información y la información que este gestiona impacta negativamente de manera leve al proceso evaluado.	La ausencia del activo de información y la información que este gestiona impacta negativamente de manera leve al proceso evaluado.
2	MEDIA	El acceso no autorizado al activo de información y a la información que este gestiona impacta negativamente al proceso evaluado.	La pérdida de la exactitud y el estado completo del activo de información y la información que este gestiona impacta negativamente al proceso evaluado.	La ausencia del activo de información y la información que este gestiona impacta negativamente al proceso evaluado.

3	**ALTA**	El acceso no autorizado al activo de información y a la información que este gestiona impacta negativamente a la entidad.	La pérdida de la exactitud y el estado completo del activo de información y la información que este gestiona impacta negativamente a la entidad.	La ausencia del activo de información y la información que este gestiona impacta negativamente a la entidad.

5.6. Clasificación de activos

Cada activo debe tener una clasificación o pertenecer a un determinado grupo de activos según su naturaleza cómo, por ejemplo: Información, Software, Hardware, Componentes de Red, servicios, intangibles, personas e instalaciones, entre otros.

El siguiente cuadro valoración de activos refleja el nivel de valoración dado a cada uno de los activos identificados de acuerdo con los pilares de seguridad de la información valorados. Anexo N°3 Valoración de activos.

6. ANALISIS DE RIESGOS

Ante una amenaza potencial podemos ahora establecer un análisis con base en los parámetros de la frecuencia y el valor de la vulnerabilidad. La probabilidad con la cual cada amenaza afectará a cada uno de los activos, y al mismo tiempo el impacto que este generará sobre los mismos.

6.1. Definición de niveles de evaluación de impacto

Para esta actividad se han definido parámetros de evaluación acordes a lo establecido en la Guía para la administración del riesgo y el diseño de controles en entidades públicas. DAFP. agosto 2025, los siguientes parámetros fueron tomados como base de clasificación.

- **Nivel Cualitativo**: es el nivel asignado a cada valor de impacto de acuerdo con la afectación financiera.
- **Nivel Cuantitativo:** define los parámetros de medición de impacto.
- **Criterios de clasificación de impacto:** define los parámetros que se tuvieron en cuenta como criterios para clasificación los mismos.

Tabla 3 Niveles de impacto

Nivel cualitativo	Nivel cuantitativo	Criterios de clasificación de impacto			
		Financiero	**Continuidad**	**Imagen**	**Legal**
		La pérdida de ingresos directa y los costos u otros gastos financieros indirectos que se generarían para la entidad.	Tiempo en que se ve afectada la operación de los procesos de la entidad.	Afectación sobre la imagen y reputación de la entidad.	Emisión de resoluciones administrativas y/o judiciales por el incumplimiento de normas, regulaciones u obligaciones.
Insignificante	**1**	Si el hecho llegara a presentarse, la entidad no tendría consecuencias económicas que impacten el funcionamiento, por tanto, se asumirán las perdidas.	Si el hecho llegara a presentarse, el proceso de la entidad no se vería afectado en su continuidad.	Si el hecho llegara a presentarse, tendría consecuencias o efectos sobre un grupo de funcionarios de manera interna.	Si el hecho llegara a presentarse, la entidad tendría multas.
Menor	**2**	Si el hecho llegara a presentarse, la entidad tendría bajas consecuencias económicas.	Si el hecho llegara a presentarse, el proceso de la entidad se vería afectado en su continuidad de manera mínima.	Si el hecho llegara a presentarse, tendría un impacto leve en la entidad que sería reparable a corto plazo	Si el hecho llegara a presentarse, la entidad tendría demandas.
Moderado	**3**	Si el hecho llegara a presentarse, la entidad tendría medianas consecuencias económicas.	Si el hecho llegara a presentarse, el proceso de la entidad se vería afectado en su continuidad de manera moderada.	Si el hecho llegara a presentarse, tendría un impacto medio en la entidad de manera local.	Si el hecho llegara a presentarse, la entidad tendría una investigación disciplinaria.
Mayor	**4**	Si el hecho llegara a presentarse, la entidad tendría altas consecuencias económicas.	Si el hecho llegara a presentarse, el proceso de la entidad se vería afectado en su continuidad de manera considerable interrumpiendo periódicamente el proceso y otros.	Si el hecho llegara a presentarse, tendría un impacto alto en la entidad a nivel gremial.	Si el hecho llegara a presentarse, la entidad tendría una investigación fiscal.
Catastrófico	**5**	Si el hecho llegara a presentarse, la entidad tendría nefastas consecuencias económicas.	Si el hecho llegara a presentarse, el proceso de la entidad se vería afectado en su continuidad de manera total.	Si el hecho llegara a presentarse, tendría un impacto catastrófico en la entidad a nivel nacional/ internacional.	Si el hecho llegara a presentarse, la entidad tendría sanciones legales. Podría generar el cierre definitivo de la entidad.

6.2. Determinación de la probabilidad

Los niveles de probabilidad definidos significan la posibilidad de materialización de un riesgo sobre determinado activo en un tiempo específico, estos al igual que el punto 5.1 fueron definidos con base en la Guía para la administración del riesgo y el diseño de controles en entidades públicas. DAFP. Agosto 2025.

Tabla 4 Niveles de probabilidad

Nivel de Probabilidad		Descripción
1	Raro	El riesgo ocurre rara vez en la entidad.
2	Improbable	El riesgo ocurre en ocasiones especificas en la entidad.
3	Posible	El riesgo ocurre con cierta periodicidad en la entidad.
4	Probable	El riesgo ocurre frecuentemente en la entidad.
5	Casi Seguro	El riesgo ocurre inminentemente en la entidad.

6.3. Identificación de amenazas por activo

Se realiza la valoración de las amenazas que permita evaluar el grado de impacto al activo por medio de los criterios definidos en el cuadro Criterios de clasificación de amenazas.

Tabla 5 Criterios de clasificación de amenazas

Niveles de Clasificación	Impacto (consecuencias) Cualitativo
Catastrófico	• Interrupción de las Operaciones de la entidad por más de cinco (5) días. • Intervención por parte de un ente de control o un ente regulador. Pérdida de información crítica para la entidad que no se puede recuperar. Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. • Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.
Mayor	• Interrupción de las Operaciones de la entidad por más de dos (2) días. • Perdida de información crítica que puede ser recuperada de forma parcial o incompleta. • Sanción por parte de entes de control u otro ente regulador. Incumplimiento en la meta y objetivos institucionales afectando el cumplimiento en las metas de gobierno. • Imagen institucional afectada en el orden nacional o regional por incumplimiento en la presentación del servicio a los usuarios o ciudadanos.

Niveles de Clasificación	Impacto (consecuencias) Cualitativo
Moderado	• Interrupción de las operaciones de la entidad por un (1) día. Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. • Inoportunidad en la información ocasionando retrasos en la atención a los usuarios. • Reproceso de actividades y aumento de carga operativa. Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. • Investigaciones penales fiscales o disciplinarias.
Menor	• Interrupción de las operaciones de la entidad por algunas horas. • Reclamaciones o quejas de los usuarios que implican investigaciones internas disciplinarias. • Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.
Insignificante	• No hay interrupción en las operaciones de la entidad. • No se generan sanciones económicas o administrativas. • No se afecta la imagen institucional de forma significativa.

Luego, se realiza la identificación de activos y amenazas que pueden impactar su funcionamiento, esto se realiza dependiendo de su valor de impacto y probabilidad.

6.4. Evaluación de riesgos

Una vez que se ha determinado el valor de riesgo para cada amenaza, que puede afectar a un activo de información, se debe tomar en primer lugar la definición de los criterios aceptables del riesgo. En otras palabras, se tiene que designar qué niveles de riesgos son asumibles y cuales deberán tomar medidas. Para tal efecto se han definido 4 niveles de riesgo para establecer los criterios de tratamiento o aceptación de riesgos según las puntuaciones posibles que se determinan en la tabla Criterios de clasificación de riesgo.

Tabla 6 Criterios de clasificación de riesgo

Niveles de riesgo	Respuesta a los riesgos	Descripción
Bajo	**Asumir el riesgo**	El nivel de riesgo es aceptable y se encuentra controlado en la entidad. Los riesgos en este nivel se deben revisar periódicamente.
Moderado	**Asumir el riesgo**	El nivel de riesgo es moderado de acuerdo con los criterios de aceptación de la entidad. Los riesgos en este nivel deben ser monitoreados para identificar oportunamente los cambios en su valoración. El riesgo ocurre rara vez en la entidad.
Alto	**Mitigar el riesgo, Evitar, Compartir**	El nivel del riesgo es alto, por lo que es necesario implementar controles en la entidad para mitigar, evitar o compartir el riesgo y llevar a niveles aceptables.

Niveles de riesgo	Respuesta a los riesgos	Descripción
Extremo	**Mitigar el riesgo, Evitar, Compartir**	El nivel del riesgo es extremo, por lo que es necesario implementar controles en la entidad para mitigar, evitar o compartir el riesgo y llevar a niveles aceptables.

Con base en los hallazgos del análisis de riesgos, el siguiente paso en el proceso es identificar las medidas que buscan disminuir los diversos niveles de riesgo. Estos se denominan dentro de la norma ISO/IEC 27001:2022 como controles de riesgos para la seguridad de la información.

6.5. Mapa de riesgos

De acuerdo con los resultados obtenidos y empleando la fórmula para valoración del riesgo la cual es dada de la siguiente manera **(Riesgo = Impacto x probabilidad)**, y según formato para el manejo del mapa de riesgos de seguridad digital. Los resultados obtenidos se representan en un mapa de calor, con el análisis de la probabilidad e impacto que tienen las amenazas identificadas para cada uno de los activos; gráfico en el cual, se representan las zonas de riesgo y se asume una posición de tratamiento. Anexo N°4 Mapa General de calor.

Zona de riesgo Baja: Asumir el riesgo
Zona de riesgo Moderada: Asumir el riesgo, Reducir el riesgo
Zona de riesgo Alta: Reducir el riesgo, Evitar, Compartir o Transferir
Zona de riesgo Extrema: Reducir el riesgo, Evitar, Compartir o Transferir

Basado en este análisis para los activos de información, desde la OTIC se realizarán mesas de trabajo con los líderes de proceso, para socializar la metodología con las áreas responsables de los procesos de la SED, para que, de acuerdo con la valoración de activos, efectúen un análisis de las amenazas detectadas en sus activos, identifique el nivel de riesgo y se establezcan controles para su tratamiento.

7. PLAN DE TRATAMIENTO DE RIESGOS

Una vez identificado los activos importantes desde el proceso de Gestión de Tecnologías de Información y comunicaciones, y realizado el análisis de riesgo para cada uno de los activos identificados por proceso, se ha diseñado un plan de tratamiento de riesgos acorde a cada una de las necesidades. Este plan de tratamiento de riesgos le permitirá a la SED definir cómo tratar el riesgo adecuadamente.

El costo/beneficio del tratamiento es un factor decisivo y relevante. La forma de opciones de tratamiento de riesgo se describe en el siguiente cuadro.

Tabla 7 Opciones tratamiento de riesgo

Costo – beneficio	Opción de tratamiento
El nivel de riesgo está muy alejado del nivel de tolerancia, su costo y tiempo del tratamiento es muy superior a los beneficios	**Evitar** el riesgo, su propósito es no proceder con la actividad o la acción que da origen al riesgo.
El costo del tratamiento por parte de terceros (internos o externos) es más beneficioso que el tratamiento directo.	**Transferir o compartir** el riesgo, entregando la gestión del riesgo a un tercero.
El costo y el tiempo del tratamiento es adecuado a los beneficios.	**Reducir o Mitigar** el riesgo, seleccionando e implementando los controles o medidas adecuadas que logren que se reduzca la probabilidad o el impacto.
La implementación de medidas de control adicionales no generará valor agregado para reducir niveles de ocurrencia o de impacto.	**Asumir** el riesgo, no se tomará la decisión de implementar medidas de control adicionales. Monitorizarlo para confirmar que no se incrementa.

7.1. Aplicación de controles

Los riesgos inherentes se han ubicado en las zonas de riesgo que requieran tratamiento; sobre los cuales, se establecen los controles para garantizar una reducción hasta un nivel aceptable para la SED. Con el fin de verificar esta eficiencia se debe realizar un monitoreo continuo y periódico para establecer la eficacia puesto que estos pueden producir resultados inesperados que deberán ser corregidos y la SED pueda tomar la decisión de aceptar, mitigar, transferir o evitar. Anexo N°4 Mapa General de calor.

7.2. Seguimiento, Monitoreo y Control

El seguimiento de los controles planteados para cada uno de los riesgos de seguridad digital y de seguridad de la información identificados se realizará por el líder de cada uno de los procesos, como primera línea de defensa, en razón a que la ubicación de los riesgos identificados después de la implementación de los controles debe estar en los niveles bajo y moderado o se deben replantear los controles.

La OTIC realizará el monitoreo de los seguimientos y los cambios que se puedan producir en los diferentes riesgos y los factores que identifiquen los procesos (activos, vulnerabilidades, amenazas, etc.), de manera semestral, y realizará modificaciones o adiciones a tiempo, según enfoque de la metodología adoptado y dependiendo de los cambios que sean identificados e informados por sus responsables. Estos cambios deben ser solicitados por el líder de cada proceso, como segunda línea de defensa.

La evaluación y control al mapa de riesgos de Seguridad Digital de la SED, lo realizará la Oficina de Control Interno, como tercera línea de defensa, en los tiempos que sean definidos desde la Política de Administración de Riesgos que establece la Oficina Asesora de Planeación.

Tabla 8 Seguimiento y Control

RESPONSABLE POR ETAPA /LINEA DE DEFENSA	ACTIVIDADES	PERIODO DE EABORACION / REPORTE	
RESPONSABLE ELABORACION **Primera Línea de defensa** **Líder y responsable de los procesos.**	1. Elaboración / Actualización Mapa de Riesgos de Seguridad Digital: Se identifica el Riesgo de Seguridad Digital (según Contexto Estratégico, Valoración de activos de información y de riesgos de seguridad digital)	Periodo de elaboración: Anual y durante el primer semestre.	
	2. Seguimiento de riesgos de Seguridad Digital y seguridad de la información y reporte a OTIC	**Periodo de seguimiento** 1. Marzo - junio 2. Julio - diciembre	**Fecha Reporte** 22/07/2026 22/01/2027
RESPONSABLE MONITOREO **Segunda Línea de defensa** **OTIC – Líder de la Política de Seguridad Digital**	1. Monitoreo a la elaboración del mapa de riesgos de seguridad digital elaborado por líderes de procesos	**Primer monitoreo:** 30 /07/2026 **Segundo monitoreo:** 31/01/2027	
RESPONSABLE DE EVALUACION Y CONTROL **Tercera Línea de defensa** **Oficina de Control Interno**	1. Revisar que se hayan identificado los riesgos significativos de seguridad digital que pueden afectar el cumplimiento de los objetivos de los procesos 2. Hacer seguimiento a las actividades del control establecidas para mitigar riesgos de seguridad digital de los procesos de la SED.	Anual según cronograma definido por la OCI para el seguimiento de la política de Administración del Riesgos de la SED	

Firma:

MILENA DEL PILAR SANDOVAL GÓMEZ
Jefe Oficina de Tecnología de la información y las Comunicaciones - OTIC

Elaborado: Juan Carlos Parra Moreno
Oficial Seguridad Digital OTIC

Revisado: Henry Alexander Moyan
Oficial Seguridad de la Información OTIC

Revisado: Jasson Smith Castro
Profesional Especializado OTIC

Revisado: Luz Dary Vargas Suarez
Profesional Especializado OTIC

ANEXO N° 1 VALORACIÓN DE ACTIVOS

Tabla 9 Valoración de activos

ID Activo	Valoración		
	Conf.	Int.	Disp.
1SW	3	3	3
2SW	3	3	3
18SW	3	3	3
19SW	3	3	3
20SW	3	3	3
21SW	3	3	3
28Datos	3	3	3
30Datos	2	3	3
34Datos	3	3	3
35Datos	2	3	3
39Datos	2	3	3
43SW	3	3	3
47SW	2	3	3
53Datos	1	3	3
54Datos	1	3	3
55Datos	1	3	3
56Datos	1	3	3
57Datos	1	3	3
58Datos	1	3	3
63Datos	3	3	3
65Datos	1	3	3
66SW	3	3	3
71HW	3	3	3
72SW	3	3	3
73HW	3	3	3
74SW	3	3	3
77HW	3	3	3
81COM	3	2	3
82COM	3	2	3
86SW	3	3	3
91SW	2	3	3
92SW	2	3	3
93SW	3	3	3
94SW	3	3	3
96SW	3	3	3
99Datos	2	3	3
113SW	3	3	3
118Datos	3	3	3
126SW	2	3	3

ID Activo	Valoración		
	Conf.	Int.	Disp.
136Datos	3	3	3
137Datos	3	3	3
142Datos	3	3	3
143Datos	3	3	3
144Datos	3	3	3
145Datos	3	3	3
146Datos	3	3	3
147Datos	3	3	3
149Datos	3	3	3
150Datos	3	3	3
151Datos	3	3	3
152SW	3	3	3
153Datos	3	3	3
154Datos	3	3	3
174SW	3	3	3
272Datos	3	3	2
288Datos	3	3	3
305Serv.	3	3	3

ANEXO N° 2 ACTIVOS DE INFORMACIÓN

Tabla 10 Activos de Información

ID_Activo	Nombre	Descripción	Tipo Activo
1SW	Aplicativo de Horas extras Docentes	Sistema de información para el reporte de horas extras de los docentes por parte de las DILES	SW
2SW	Share point Fallos Judiciales	Sistema de información para realizar seguimiento al estado del trámite de la liquidación y pago de los fallos judiciales	SW
18SW	SIAPI	Registrar la atención integral a la primera infancia que tiene como objetivo principal brindar educación de calidad a las niñas y niños garantizando el cumplimiento de todos los aspectos necesarios para su desarrollo integral	SW
19SW	SVDI - Sistema de Valoración al Desarrollo Infantil	El Sistema de Valoración del Desarrollo Integral (SVDI) es un sistema que se implementará en Bogotá para generar información sobre la atención integral.	SW
20SW	Monitoreo y seguimiento	Permite realizar una consolidación del monitoreo y la calidad educativa en todos los aspectos para el desarrollo integral de la Primera Infancia.	SW
21SW	SIMECONOCES	El sistema de información permite realizar la consolidación, seguimiento y control de la información de las atenciones que brindan las entidades aliadas, sector cultura y cajas de compensación dentro de los procesos de Jornadas Única y Complementaria.	SW
28Datos	Títulos valores convenio APICE	Corresponde a los títulos valores (pagarés) suscritos por los beneficiarios del Convenio de Asociación 1973-2009 APICE que respaldan las obligaciones contraídas por estos para la financiación de programas académicos cursados en los niveles técnico profesional, tecnológico o universitario.	Datos
30Datos	Actas de la Junta Directiva del Fondo Distrital para la Financiación de la Educación Superior — Educación Superior para Todos (FEST)	Las Actas de la Junta Directiva del Fondo Distrital para la Financiación de la Educación Superior — Educación Superior para Todos (FEST) evidencina la creación y conformación de este órgano de dirección y, adicionalmente, son la memoria de las deliberaciones, acciones y decisiones que se toman internamente, en cumplimiento de las funciones establecidas en el artículo 71 del Decreto Distrital 421 de 2019, para responder a los retos que la ciudad demanda en materia de acceso a la educación superior y educación para el trabajo y desarrollo humano.	Datos
34Datos	Historias de beneficiarios del Fondo Distrital para la Financiación de la Educación Superior — Educación Superior para Todos (FEST)	Subserie documental que contiene soportes de los procesos individuales de los beneficiarios, desde su ingreso al programa hasta la finalización de sus estudios, proporcionando una visión detallada y estructurada del seguimiento y control de los recursos destinados a financiar a través de un crédito beca condonable hasta del 100% su formación en los niveles técnico profesional, tecnológico o profesional universitario	Datos
35Datos	Actas del Comité de Becas	Subserie documental que recopila los registros de las sesiones realizadas por el Comité de Becas de la Secretaría de Educación del Distrito, creado mediante la Resolución 2142 del 15 de diciembre de 2017. Este comité, cuya secretaría técnica está a cargo de la Dirección de Relaciones con los Sectores de Educación Superior y Educación para el Trabajo y tiene como propósito principal establecer y supervisar los criterios y requisitos para la asignación de becas otorgadas por la Universidad Libre de Colombia y la Fundación Universidad de América, en cumplimiento de los Acuerdos Distritales 14 de 1958 y 17 de 1963	Datos

ID_Activo	Nombre	Descripción	Tipo Activo
39Datos	Organismos de control	La subserie documental Programa de Portafolio de Becas evidencia la implementación de las Políticas Públicas orientadas a fomentar las oportunidades de acceso a la educación superior de los mejores bachilleres matriculados en el Sistema Educación Oficial del Distrito, así como diseñar y coordinar las estrategias desarrolladas por los fondos de financiamiento para la educación superior y gestionar otras acciones que promuevan el acceso y permanencia en el sistema educativo. Los tiempos de retención asignados a esta agrupación documental se aplicarán a partir del momento en que tenga lugar el reconocimiento y desembolso de las becas otorgadas por la entidad a los beneficiarios del programa. Cumplido el tiempo de retención en cada una de las fases de archivo, la subserie documental se deberá realizar una selección cualitativa de la documentación de acuerdo con la disposición anual en el proceso de asignación del Programa del Portafolio de Becas	Datos
43SW	Alertas	Permite a los colegios del Distrito reportar y realizar seguimiento a los eventos o situaciones de presunta vulneración de los derechos de las niñas, niños y jóvenes que se presentan en el interior de los colegios o fuera de estos.	SW
47SW	SACE-Sistema de Alianzas y Cooperación Escolar	Sistema para registrar y gestionar las alianzas y/o acuerdos de cooperación escolar.	SW
53Datos	Circulares	Serie documental que reúne el consecutivo de actos administrativos expedidos por el Secretario de Despacho y las Subsecretarías de la entidad, con el propósito de brindar información sobre asuntos relacionados con el desarrollo e integración de las políticas del sector educativo y el fortalecimiento de relaciones interinstitucionales de la entidad, solicitar información a las entidades u organismos distritales o difundir asuntos de interés hacia la ciudadanía	Datos
54Datos	Conceptos de Proyectos de Acuerdo	Subserie documental integrada por los conceptos emitidos por la Oficina Asesora Jurídica de la Secretaría de Educación del Distrito, como respuesta a las peticiones realizadas en ejercicio del derecho de petición de consulta consagrado en el artículo 23 de la Constitución Política de Colombia y desarrollado en el artículo 14 y siguientes del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, donde se refleja la interpretación jurídica de la entidad frente a un tema o asunto relacionado con las funciones a su cargo	Datos
55Datos	Proposiciones de control Político	Serie documental conformada por las comunicaciones recibidas y emitidas en función de la revisión y respuesta a los cuestionarios presentados por el Concejo de Bogotá o el Congreso de la República, para ejercer control político sobre las políticas del sector educativo, y el uso transparente y eficiente de los recursos públicos de la entidad	Datos
56Datos	Resoluciones	Serie documental que reúne el consecutivo de actos administrativos expedidos por las unidades administrativas productoras, mediante los cuales se define o resuelve situaciones de carácter particular y concreto, se reglamentan decretos o acuerdos diferentes a los expedidos por el Concejo de Bogotá o se desarrollan funciones específicas de la entidad	Datos
57Datos	Autos	Serie documental que reúne el consecutivo de actos administrativos que se emiten en el curso de un	Datos

ID_Activo	Nombre	Descripción	Tipo Activo
		procedimiento disciplinario. Puede ser de reconocimiento de personería jurídica a representante legal, investigación, inhibitorio o de terminación y/o archivo	
58Datos	Actas de los Comités Directivos	Las actas del Comité constarán por escrito, numeradas en forma consecutiva y contendrán los aspectos discutidos en cada sesión, así como las recomendaciones realizadas por los miembros, en caso de que haya lugar	Datos
63Datos	Bases de Datos en Excel	Herramienta que permite organizar, recopilar información y generar trazabilidad de los documentos de asunto político (proposiciones del Concejo, proyectos de acuerdo del Concejo, proyectos de Ley Concejo y Congreso, Juntas Administradoras Locales, congreso, derechos petición Concejo de Bogotá, entre otros)	Datos
65Datos	Autorización para la suscripción de contratos con objetos iguales	Se refiere a documento a través del cual se autoriza la celebración de contratos, convenios o procesos que tienen el mismo objeto contractual, es decir, la misma finalidad, actividad o servicio	Datos
66SW	Base de datos de control	Se registran todos los procesos de segunda instancia disciplinaria que se remiten a la OAJ - En esta base de datos se registra toda la información relevante de los expedientes que fueron enviados a esta Oficina. - Dicha base fue creada para registrar cada uno de los procesos donde se ha proferido una decisión de fondo por parte de este despacho.	SW
71HW	Firewall Perimetrales CDI-NVC	Dispositivo On Premise, cuyo propósito especifico es la protección perimetral de la red del datacenter principal de la SED.	HW
72SW	Firewall Virtuales Cloud Oracle - Azure	Servicio SAS, cuyo propósito especifico es la protección perimetral de la red privada de Oracle para los servicios alojados por la SED.	SW
73HW	Firewall WEB CDI - CTD	Dispositivo On Premise, cuyo propósito especifico es la protección a nivel de capa de aplicación de los servicios WEB publicados y alojados en el datacenter On Premise principal de la SED.	HW
74SW	Firewall WEB Virtual Cloud Oracle - Azure	Servicio SAS, cuyo propósito especifico es la protección a nivel de capa de aplicación de los servicios WEB publicados y alojados en la nube de Oracle.	SW
77HW	Gateway de Correo	Dispositivo On Premise, cuyo propósito especifico es el de proteger el servicio de correo de la SED.	HW
81COM	Canales de comunicación público (Internet)	Canales de comunicación entre las nubes privadas (Oracle y Azure) y datacenter principal de la SED.	COM
82COM	Canales de comunicación WAN	Canal de comunicación entre las sedes de NVC y CDI	COM
86SW	Sistema de Apoyo Escolar	Sistema de Información que permite a los colegios optimizar la gestión operativa que se desarrolla alrededor de los procesos académicos de los estudiantes y que les da la posibilidad de ser autónomos en la generacion e impresión de los reportes académicos.	SW
91SW	DHCP	(Protocolo de Configuración Dinámica de Host) es un protocolo de red que asigna automáticamente direcciones IP, máscaras de subred, puertas de enlace y DNS a los dispositivos.	SW
92SW	DNS	(Sistema de Nombres de Dominio) es la «agenda telefónica» de Internet. Traduce nombres de dominio legibles por humanos (ej. google.com) a direcciones IP numéricas (ej. 74.125.19.147) que los equipos usan para conectarse, permitiendo navegar por la web sin recordar números complejos.	SW
93SW	Controlador de Dominio	(DC) es un servidor crítico en redes, principalmente Windows Active Directory (AD), que autentica usuarios y	SW

ID_Activo	Nombre	Descripción	Tipo Activo
		equipos, gestiona permisos y aplica políticas de seguridad.	
94SW	Alertas	Permite a los colegios del Distrito reportar y realizar seguimiento a los eventos o situaciones de presunta vulneración de los derechos de las niñas, niños y jóvenes que se presentan en el interior de los colegios o fuera de estos.	SW
96SW	GeoVisor - Una herramienta del Comité Distrital de Convivencia Escolar	Herramienta tecnológica que usa datos geoespaciales institucionales e interinstitucionales enfocado en entornos escolares, lo cual permite hacer análisis territoriales para la toma de decisiones informadas	SW
99Datos	BD Resultados evaluaciones externas	Archivo en formato Access que contiene los resultados consolidados de las pruebas externas que se aplican en la ciudad, incluyen: - Examen Saber 11 desde 2000 a 2025 - Pruebas 3°, 5° y 9° desde 2009 a 2017 - Índice Sintético de Calidad ISCE desde 2015 a 2018 - Pruebas PISA desde 2009 a 2022	Datos
113SW	SIMECONOCES	El sistema de información permite realizar la consolidación, seguimiento y control de la información de las atenciones que brindan las entidades aliadas, sector cultura y cajas de compensación dentro de los procesos de Jornadas Única y Complementaria.	SW
118Datos	Repositorio documental Formación Docente	Permite tener acceso desde el SharePoint de la dirección de formación docente a documentos técnicos, actas de reuniones, resultados finales e informes generales de los diferentes convenios y procesos que se manejan con la intención de beneficiar a las direfentes instituciones educativas del distrito.	Datos
126SW	Sistema Koha de las Bibliotecas Escolares	Herramienta on line para la gestión y control de bibliotecas de los colegios del Distrito, permite generar una interacción entre las bibliotecas, bibliotecarios, docentes, estudiantes.	SW
136Datos	Certificaciones	Serie documental conformada por los documentos generados en función de las solicitudes realizadas por los funcionarios de la Secretaría de Educación del Distrito para acreditar experiencia laboral, salario devengado, cargo y funciones desempeñadas, entre otras situaciones administrativas generadas en virtud de la relación laboral con la entidad.	Datos
137Datos	Contratos en General	Subserie documental en la que se agrupa la documentación que soporta la elaboración, trámite y ejecución del proceso de contratación directa, por el cual un tercero, sea esta una persona jurídica o natural, se obliga a transferir temporalmente el uso y goce de bien inmueble a la Secretaría de Educación del Distrito.	Datos
142Datos	Share point Horas Extras	Cargar todas las Ordenes de Servicio que se aprobaron en DILE para efectos de pago ante la oficina de nómina.	Datos
143Datos	Share point documentación DILE	Cargar todos los archivos digitales que en el ejercicio como servidor público se genera desde el rol de talento humano.	Datos
144Datos	Asesorar y orientar a los rectores de los colegios (oficios, correos electrónicos y telefónicamente)	Brindar asesoría a los rectores para la toma de decisiones que en relación con procesos de talento humano refieran	Datos
145Datos	Proceso de encargos de directivos docentes	Revisar las necesidades que por este concepto se generen aplicando parámetros normativos y solicitar ante oficina de personal la apertura del proceso	Datos

ID_Activo	Nombre	Descripción	Tipo Activo
	(correos, archivos Excel)		
146Datos	Respuestas a entes de control, despachos judiciales y ciudadanía en general (oficios-correos electrónicos)	Atender todas las solicitudes que sean allegadas por entes de control y ciudadanía relacionados con los procesos de talento humano	Datos
147Datos	necesidades de personal administrativo-informes-seguimiento control-correos electrónicos-oficios-otros	validar y atender todas las necesidades de personal administrativo y directivo docente que se presentan en las IED de la DILE	Datos
149Datos	Convenios	Serie documental en la que se agrupa la documentación que soporta los convenios de asociación celebrados entre la Secretaría de Educación del Distrito y personas jurídicas públicas o privadas, mediante los cuales las partes establecen acuerdos de cooperación mutua para desarrollar actividades de interés y beneficio común.	Datos
150Datos	Informes a Entidades de Control y Vigilancia	Subserie documental constituida por los documentos que soportan la elaboración y trámite de los informes requeridos por las entidades gubernamentales que tienen como misión hacer control sobre la gestión de las entidades públicas y particulares que ejerzan funciones públicas, tales como la Contraloría General de la República, la Contraloría Distrital, la Procuraduría General de la Nación, la Personería de Bogotá y la Veeduría Distrital.	Datos
151Datos	Base de datos Herramienta de gestión Dirección de Contratación	Base de datos de la información contractual de la entidad	Datos
152SW	Herramienta de gestión Dirección de Contratación	Aplicativo contratos	SW
153Datos	Informes a Otros Organismos de Control y Vigilancia	Subserie documental constituida por los documentos que soportan la elaboración y trámite de los informes requeridos por las entidades gubernamentales que tienen como misión hacer control sobre la gestión de las entidades públicas y particulares que ejerzan funciones públicas, tales como la Contraloría General de la República, la Contraloría Distrital, la Procuraduría General de la Nación, la Personería de Bogotá y la Veeduría Distrital.	Datos
154Datos	Plan Anual de Adquisiciones - PAA	Subserie documental que contiene la proyección de los bienes y servicio requeridos por la Secretaría de Educación del Distrito durante cada vigencia fiscal, consolidando toda la información clave relacionada con las necesidades de compra de la entidad de manera organizada y estructurada; con el fin de atender las necesidades establecidas por la entidad para la ejecución de los fines y objetivos institucionales, bajo los principios de eficiencia, eficacia y transparencia en el uso de los recursos.	Datos
174SW	Portal Web Secretaria de	Portal de divulgación de información De la Secretaria de Educación del Distrito	SW

ID_Activo	Nombre	Descripción	Tipo Activo
	Educación del Distrito		
272Datos	Actas de Comité de Convivencia y Conciliación Laboral	Son documentos oficiales que registran las reuniones del Comité de Convivencia Laboral, en las cuales se analizan situaciones relacionadas con el clima organizacional, conflictos laborales y posibles casos de acoso laboral, dejando constancia de los acuerdos, recomendaciones y acciones de conciliación orientadas a promover relaciones laborales respetuosas y un ambiente de trabajo sano.	Datos
288Datos	Actas de Comité de Convivencia y Conciliación Laboral	Dentro de esta subserie se encuentra registrada las decisiones tomadas y las acciones implementadas para la aplicación de las políticas nacionales de prevención y corrección del acoso laboral	Datos
305Serv.	Servicios de Microsoft365 (One Drive, SharePoint, etc.)	suite de productividad basada en la nube que incluye aplicaciones esenciales como Word, Excel, PowerPoint, Outlook, OneNote y Teams, junto con almacenamiento en la nube OneDrive y SharePoint.	Serv.

ANEXO N° 3 VALORACIÓN DE ACTIVOS

Tabla 11 Valoración de activos

ID	Nombre	Tipo Activo	Nivel de criticidad
1SW	Aplicativo de Horas extras Docentes	SW	ALTA
2SW	Share point Fallos Judiciales	SW	ALTA
18SW	SIAPI	SW	ALTA
19SW	SVDI - Sistema de Valoración al Desarrollo Infantil	SW	ALTA
20SW	Monitoreo y seguimiento	SW	ALTA
21SW	SIMECONOCES	SW	ALTA
28Datos	Títulos valores convenio APICE	Datos	ALTA
30Datos	Actas de la Junta Directiva del Fondo Distrital para la Financiación de la Educación Superior — Educación Superior para Todos (FEST)	Datos	ALTA
34Datos	Historias de beneficiarios del Fondo Distrital para la Financiación de la Educación Superior — Educación Superior para Todos (FEST)	Datos	ALTA
35Datos	Actas del Comité de Becas	Datos	ALTA
39Datos	Organismos de control	Datos	ALTA
43SW	Alertas	SW	ALTA
47SW	SACE-Sistema de Alianzas y Cooperación Escolar	SW	ALTA
53Datos	Circulares	Datos	ALTA
54Datos	Conceptos de Proyectos de Acuerdo	Datos	ALTA
55Datos	Proposiciones de control Político	Datos	ALTA
56Datos	Resoluciones	Datos	ALTA
57Datos	Autos	Datos	ALTA
58Datos	Actas de los Comités Directivos	Datos	ALTA
63Datos	Bases de Datos en Excel	Datos	ALTA
65Datos	Autorización para la suscripción de contratos con objetos iguales	Datos	ALTA
66SW	Base de datos de control	SW	ALTA
71HW	Firewall Perimetrales CDI-NVC	HW	ALTA
72SW	Firewall Virtuales Cloud Oracle - Azure	SW	ALTA
73HW	Firewall WEB CDI - CTD	HW	ALTA
74SW	Firewall WEB Virtual Cloud Oracle - Azure	SW	ALTA
77HW	Gateway de Correo	HW	ALTA
81COM	Canales de comunicación público (Internet)	COM	ALTA
82COM	Canales de comunicación WAN	COM	ALTA
86SW	Sistema de Apoyo Escolar	SW	ALTA
91SW	DHCP	SW	ALTA
92SW	DNS	SW	ALTA
93SW	Controlador de Dominio	SW	ALTA
94SW	Alertas	SW	ALTA
96SW	GeoVisor - Una herramienta del Comité Distrital de Convivencia Escolar	SW	ALTA
99Datos	BD Resultados evaluaciones externas	Datos	ALTA
113SW	SIMECONOCES	SW	ALTA
118Datos	Repositorio documental Formación Docente	Datos	ALTA
126SW	Sistema Koha de las Bibliotecas Escolares	SW	ALTA
136Datos	Certificaciones	Datos	ALTA
137Datos	Contratos en General	Datos	ALTA
142Datos	Share point Horas Extras	Datos	ALTA
143Datos	Share point documentación DILE	Datos	ALTA
144Datos	Asesorar y orientar a los rectores de los colegios (oficios, correos electrónicos y telefónicamente)	Datos	ALTA
145Datos	Proceso de encargos de directivos docentes (correos, archivos Excel)	Datos	ALTA
146Datos	Respuestas a entes de control, despachos judiciales y ciudadanía en general (oficios-correos electrónicos)	Datos	ALTA

ID	Nombre	Tipo Activo	Nivel de criticidad
147Datos	necesidades de personal administrativo-informes-seguimiento control-correos electrónicos-oficios-otros	Datos	ALTA
149Datos	Convenios	Datos	ALTA
150Datos	Informes a Entidades de Control y Vigilancia	Datos	ALTA
151Datos	Base de datos Herramienta de gestión Dirección de Contratación	Datos	ALTA
152SW	Herramienta de gestión Dirección de Contratación	SW	ALTA
153Datos	Informes a Otros Organismos de Control y Vigilancia	Datos	ALTA
154Datos	Plan Anual de Adquisiciones - PAA	Datos	ALTA
174SW	Portal Web Secretaria de Educación del Distrito	SW	ALTA
272Datos	Actas de Comité de Convivencia y Conciliación Laboral	Datos	ALTA
288Datos	Actas de Comité de Convivencia y Conciliación Laboral	Datos	ALTA
305Serv.	Servicios de Microsoft365 (One Drive, SharePoint, etc.)	Serv.	ALTA

ANEXO N°4 MAPA DE CALOR RIESGO INHERENTE

Tabla 12 Mapa Calor Riesgo Inherente

Probabilidad	**Muy Alta 100%**					
	Alta 80%			R185	R13, R30, R47, R64, R81 R98, R168, R279, R292, R302 R312, R322, R332, R366, R413 R430, R458, R486, R624, R663 R699	
	Media 60%		R670, R672, R673 R681, R683, R684	R175, R177, R184 R247, R249, R250	R3, R5, R6, R10, R12 R20, R22, R23, R27, R29 R37, R39, R40, R44, R46 R54, R56, R57, R61, R63 R71, R73, R74, R78, R80 R88, R90, R91, R95, R97 R105, R107, R108, R112, R116 R118, R119, R123, R127, R129 R130, R134, R138, R140, R141 R145, R148, R150, R151, R158 R160, R161, R165, R167, R192 R194, R195, R199, R203, R205 R206, R210, R214, R216, R217 R221, R225, R227, R228, R232 R236, R238, R239, R243, R258 R260, R261, R265, R269, R271 R272, R276, R278, R287, R288 R297, R298, R307, R308, R317 R318, R327, R328, R335, R339 R342, R345, R349, R352, R356 R358, R359, R363, R365, R372 R376, R379, R382, R386, R389 R392, R396, R399, R403, R405 R406, R410, R412, R420, R422 R423, R427, R429, R437, R439 R440, R444, R448, R450, R451 R455, R457, R465, R467, R468 R472, R476, R478, R479, R483 R485, R493, R495, R496, R500 R504, R506, R507, R511, R515 R517, R518, R522, R526, R528 R529, R533, R537, R539, R540 R544, R548, R550, R551, R555 R559, R561, R562, R566, R570 R572, R573, R577, R581, R583 R584, R588, R592, R594, R595	
	Baja 40%		R668, R674, R679, R685	R173, R179, R186, R189 R245, R251	R1, R7, R14, R17, R18 R24, R31, R34, R35, R41 R48, R51, R52, R58, R65 R68, R69, R75, R82, R85 R86, R92, R99, R102, R103 R109, R114, R120, R125, R131 R136, R142, R146, R152, R154 R156, R162, R169, R172, R190 R196, R201, R207, R212, R218 R223, R229, R234, R240, R256 R262, R267, R273, R280, R283 R284, R293, R294, R303, R304 R313, R314, R323, R324, R333 R338, R340, R341, R348, R350 R351, R354, R360, R367, R370 R375, R377, R378, R385, R387 R388, R395, R397, R398, R401 R407, R414, R417, R418, R424 R431, R434, R435, R441, R446 R452, R459, R462, R463, R469 R474, R480, R487, R490, R491 R497, R502, R508, R513, R519 R524, R530, R535, R541, R546 R552, R557, R563, R568, R574 R579, R585, R590, R596, R601 R607, R612, R618, R625, R628 R629, R635, R640, R646, R651 R657, R664, R667, R692, R700 R702	
	Muy Baja 20%		R669, R680	R174, R246	R2, R19, R36, R53, R70 R87, R104, R115, R126, R137 R147, R157, R191, R202, R213 R224, R235, R257, R268, R285 R286, R295, R296, R305, R306 R315, R316, R325, R326, R343 R353, R355, R380, R390, R400 R402, R419, R436, R447, R464 R475, R492, R503, R514, R525 R536, R547, R558, R569, R580 R591, R602, R613, R630, R641 R652	
		Leve 20%	**Menor 40%**	**Moderado 60%**	**Mayor 80%**	**Catastrófico 100%**
		Impacto				

ANEXO N°5 MAPA DE CALOR RIESGO RESIDUAL

Tabla 13 Mapa Calor Riesgo Residual

Probabilidad						
	Muy Alta 100%					
	Alta 80%				R4	
	Media 60%				R6	
	Baja 40%		R671, R676, R678, R682, R687 R689	R176, R183, R185, R188, R248 R253, R255	R1, R8, R11, R13, R16 R21, R28, R30, R33, R38 R45, R47, R50, R55, R62 R64, R67, R72, R79, R81 R84, R89, R96, R98, R101 R106, R111, R113, R117, R122 R124, R128, R135, R139, R149 R159, R166, R168, R171, R193 R198, R200, R204, R209, R211 R215, R220, R222, R226, R231 R233, R237, R242, R244, R259 R264, R266, R270, R277, R279 R282, R289, R292, R299, R302 R309, R312, R319, R322, R329 R332, R357, R364, R366, R369 R404, R411, R413, R416, R421 R428, R430, R433, R438, R443 R445, R449, R456, R458, R461 R466, R471, R473, R477, R484 R486, R489, R494, R499, R501 R505, R510, R512, R516, R521 R523, R527, R532, R534, R538 R543, R545, R549, R554, R556 R560, R565, R567, R571, R576 R578, R582, R587, R589, R593 R598, R600, R604, R609, R611 R615, R622, R624, R627, R632 R637, R639, R643, R648, R650 R654, R661, R663, R666, R690 R696, R699, R701	
	Muy Baja 20%		R668, R669, R670, R672, R673 R674, R675, R677, R679, R680 R681, R683, R684, R685, R686 R688	R173, R174, R175, R177, R178 R179, R181, R182, R184, R186 R187, R189, R245, R246, R247 R249, R250, R251, R252, R254	R2, R3, R5, R7, R9 R10, R12, R14, R15, R17 R18, R19, R20, R22, R23 R24, R25, R26, R27, R29 R31, R32, R34, R35, R36 R37, R39, R40, R41, R43 R44, R46, R48, R49, R51 R52, R53, R54, R56, R57 R58, R60, R61, R63, R65 R66, R68, R69, R70, R71 R73, R74, R75, R77, R78 R80, R82, R83, R85, R86 R87, R88, R90, R91, R92 R94, R95, R97, R99, R100 R102, R103, R104, R105, R107 R108, R109, R110, R112, R114 R115, R116, R118, R119, R120 R121, R123, R125, R126, R127 R129, R130, R131, R133, R134 R136, R137, R138, R140, R141 R142, R144, R145, R146, R147 R148, R150, R151, R152, R154 R156, R157, R158, R160, R161 R162, R164, R165, R167, R169 R170, R172, R190, R191, R192 R194, R195, R196, R197, R199 R201, R202, R203, R205, R206 R207, R208, R210, R212, R213 R214, R216, R217, R218, R219 R221, R223, R224, R225, R227 R228, R229, R230, R232, R234 R235, R236, R238, R239, R240 R241, R243, R256, R257, R258 R260, R261, R262, R263, R265 R267, R268, R269, R271, R272 R273, R275, R276, R278, R280	
		Leve 20%	**Menor 40%**	**Moderado 60%**	**Mayor 80%**	**Catastrófico 100%**
		Impacto				

ANEXO N°6 DEFINICIÓN DE CONTROLES

Tabla 14 Definición de Controles

Riesgo	Control de la Norma	Estrategia
R468 R623 R485 R634 R496 R645 R507 R662 R518 R673 R529 R684 R540 R697 R551 R703 R562 R584 R573 R595 R606	5.12 Control: La información debe clasificarse en función de las necesidades de seguridad de la información de la organización basadas en la confidencialidad, la integridad, la disponibilidad y los requisitos pertinentes de las partes interesadas.	La organización debe establecer una política específica sobre clasificación de la información y comunicarla a todas las partes interesadas pertinentes. Las clasificaciones y los controles de protección de la información asociados deben tener en cuenta las necesidades empresariales para compartir o restringir la información, para proteger la integridad de la información y para garantizar la disponibilidad, así como los requisitos legales relativos a la confidencialidad, integridad o disponibilidad de la información. * Los activos distintos de la información también pueden clasificarse de conformidad con la clasificación de información, que se almacena en el activo, se procesa con él o se maneja o protege de otro modo con él. * Los propietarios de la información deben ser responsables de su clasificación. * El esquema de clasificación debe incluir convenciones para la clasificación y criterios para la revisión de la clasificación a lo largo del tiempo.
R700	5.16 Control: Se gestionará el ciclo de vida completo de las identidades.	La entidad deberá definir un proceso de gestión de identidades, el cual garantice: a) para las identidades asignadas a personas, una identidad específica sólo esté vinculada a una única persona para poder responsabilizar a la persona de las acciones realizadas con esta identidad específica; b) las identidades asignadas a múltiples personas (por ejemplo, identidades compartidas) sólo se permitan cuando sean necesarias por razones empresariales u operativas y estén sujetas a aprobación y documentación específicas. documentación específica; c) las identidades asignadas a entidades no humanas están sujetas a una aprobación debidamente segregada y a una supervisión continua independiente; d) las identidades se desactiven o eliminen en el momento oportuno si ya no son necesarias (por ejemplo, si sus entidades asociadas se eliminan o ya no se utilizan, o si la persona vinculada a una identidad ha abandonado la organización o ha cambiado de función); e) en un ámbito específico, se asigna una única identidad, [es decir, se evita la asignación de múltiples identidades a la misma entidad dentro del mismo contexto (identidades duplicadas) f) se mantengan registros de todos los eventos significativos relacionados con el uso y la gestión de las identidades de usuario y de la información de autenticación.
R6 R372 R23 R382 R40 R392 R57 R406 R74 R423 R91 R451 R130 R479 R141 R617 R151 R656 R161 R691 R178 R359 R272 R345 R335	5.29 Control: La organización debe planificar cómo mantener la seguridad de la información en un nivel adecuado durante la interrupción.	La organización debe determinar sus requisitos para adaptar los controles de seguridad de la información durante la interrupción. Los requisitos de seguridad de la información deben incluirse en los procesos de gestión de la continuidad del negocio. Deben elaborarse, aplicarse, probarse, revisarse y evaluarse planes para mantener o restablecer la seguridad de la información de los procesos empresariales críticos tras una interrupción o fallo. La seguridad de la información debe restablecerse al nivel y en los plazos requeridos. La organización debe implantar y mantener a) controles de seguridad de la información, sistemas de apoyo y herramientas dentro de los planes de continuidad de

Riesgo	Control de la Norma	Estrategia
		la actividad y de las TIC; b) procesos para mantener los controles de seguridad de la información existentes durante la interrupción; c) controles compensatorios para los controles de seguridad de la información que no puedan mantenerse durante interrupción.
R16 R33 R50 R67 R84 R101 R111 R122 R171 R188 R198 R209 R220 R231 R242 R253 R264 R282 R369 R416 R433 R443 R461 R471 R489 R499 R510 R521 R532 R543 R554 R565 R576 R587 R598 R609 R627 R637 R648 R666 R676 R687 R701	5.33 Control: Los registros deben protegerse contra pérdida, destrucción, falsificación, acceso no autorizado y publicación no autorizada.	La organización debe adoptar las siguientes medidas para proteger la autenticidad, fiabilidad, integridad y facilidad de uso de los documentos de archivo, a medida que cambien con el tiempo: a) emitir directrices sobre el almacenamiento, la cadena de custodia y la eliminación de los registros, que incluyan prevención de la manipulación de documentos de archivo. Estas directrices deben estar en consonancia con la política de la organización política específica de la organización en materia de gestión de documentos y otros requisitos relativos a los documentos; b) elaborar un calendario de conservación en el que se definan los registros y el periodo de tiempo durante el cual deben conservarse. El sistema de almacenamiento y tratamiento debe garantizar la identificación de los documentos y su periodo de conservación, teniendo en cuenta la legislación o normativa nacional o regional, así como las expectativas de la comunidad o la sociedad, si procede. Este sistema debe permitir la destrucción adecuada de los documentos después de ese periodo si la organización no los necesita. A la hora de decidir sobre la protección de determinados documentos de archivo de la organización, debe tenerse en cuenta su correspondiente clasificación de seguridad de la información, basada en el esquema de clasificación de la organización. Los registros deben clasificarse en tipos (por ejemplo, registros contables, registros de transacciones comerciales, registros de personal, registros legales), cada uno con detalles sobre los periodos de conservación y el tipo de soporte de almacenamiento permitido, que puede ser físico o electrónico. Los sistemas de almacenamiento de datos deben elegirse de forma que los registros necesarios puedan recuperarse en un plazo aceptable plazo y formato, en función de los requisitos que deban cumplirse. Cuando se opte por medios de almacenamiento electrónico, deberán establecerse procedimientos que garanticen la capacidad de acceso a los registros (tanto a los medios de almacenamiento como a la legibilidad del formato) durante todo el periodo de conservación, a fin de salvaguardarlos de posibles pérdidas debidas a futuros cambios tecnológicos. También deben conservarse las claves criptográficas y los programas asociados a los archivos cifrados o a las firmas digitales, para permitir el descifrado de los documentos de archivo durante el periodo de conservación de los mismos. Los procedimientos de almacenamiento y manipulación deben aplicarse de acuerdo con las recomendaciones de los fabricantes de los medios de almacenamiento. Debe tenerse en cuenta la posibilidad de deterioro de los soportes utilizados para almacenar los documentos.
R8 R25	5.4 Control: La gerencia debe exigir a todo el personal que	Luego de un cambio de administración, la alta dirección deberá recibir capacitaciones destinadas a comprender su papel dentro de la seguridad de la información y a partir de ello definir acciones para garantizar que se conocen y se cumplen las políticas de seguridad de la información. Estas

Riesgo	Control de la Norma	Estrategia
R346 R361 R373 R383 R393 R408 R425 R453 R481 R619 R658 R694	aplique la seguridad de la información de acuerdo con la política de seguridad de la información establecida, las políticas y los procedimientos específicos del tema de la organización.	acciones deberán garantizar: 1. Que todos los contratos de prestación de servicios, así como contratos al personal de planta incluyan: * el conocimiento de funciones y responsabilidades en materia de seguridad de la información. * Mandato de cumplimiento la a política de seguridad de la información y las políticas temáticas específicas de la organización. * que se cuente con un canal confidencial para denuncia de infracciones de la política de seguridad de la información, permitiendo la denuncia anónima. 2. Garantizar que el personal responsable de seguridad de la información mantenga sus competencias mediante formación profesional continua.
R12 R261 R29 R278 R46 R338 R63 R348 R80 R365 R97 R375 R108 R385 R119 R395 R167 R412 R184 R429 R195 R440 R206 R457 R217 R693 R228 R698 R239 R699 R250	6.3 Control: El personal de la organización y las partes interesadas relevantes deben recibir la conciencia, educación y capacitación adecuadas en seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización, las políticas y los procedimientos específicos del tema, según sea relevante para su función laboral.	Debe establecerse un programa de concienciación, educación y formación en materia de seguridad de la información en consonancia con la política de seguridad de la información de la organización, las políticas específicas de cada tema y los procedimientos pertinentes sobre seguridad de la información, teniendo en cuenta la información de la organización que debe protegerse y los controles de seguridad de la información que se han implementado para proteger la información. La concienciación, educación y formación en materia de seguridad de la información deben tener lugar periódicamente. Inicialmente. La concienciación, la educación y la formación iniciales pueden aplicarse al personal nuevo y a los que se trasladan a nuevos puestos o funciones sustancialmente diferentes de la seguridad de la información. puestos o funciones con requisitos de seguridad de la información. La comprensión del personal debe evaluarse al final de una actividad de concienciación, educación o formación para comprobar la transferencia de conocimientos y la eficacia del programa de sensibilización, educación y formación.
R3 R327 R20 R356 R37 R403 R54 R420 R71 R437 R88 R448 R105 R465 R116 R476 R127 R493 R138 R504 R148 R515 R158 R526 R175 R537 R192 R548 R203 R559 R214 R570 R225 R581 R236 R592 R247 R603 R258 R614 R269 R631 R287 R642 R297 R653 R307 R670 R317 R681	7.13 Control: El equipo se mantendrá correctamente para garantizar la disponibilidad, integridad y confidencialidad de la información.	Deben tenerse en cuenta las siguientes directrices para el mantenimiento de los equipos a) mantener el equipo de acuerdo con la frecuencia de servicio recomendada por el proveedor; b) aplicación y supervisión de un programa de mantenimiento por parte de la organización; c) que sólo el personal de mantenimiento autorizado lleve a cabo las reparaciones y el mantenimiento de los equipos; d) mantenimiento de registros de todas las averías presuntas o reales y de todo el mantenimiento preventivo y correctivo; e) la aplicación de controles apropiados cuando se prevea el mantenimiento de los equipos, teniendo en cuenta si este mantenimiento lo realiza personal in situ o externo a la organización; someter al personal de mantenimiento a un acuerdo de confidencialidad adecuado; f) supervisar al personal de mantenimiento cuando realice tareas de mantenimiento in situ; g) autorizar y controlar el acceso para el mantenimiento a distancia; h) aplicar medidas de seguridad para los activos fuera de las instalaciones (véase 7.9) si el equipo que contiene la información se sacan de los locales para su mantenimiento. i) cumplir todos los requisitos de mantenimiento impuestos por los seguros;

Riesgo	Control de la Norma	Estrategia
		j) antes de volver a poner en funcionamiento el equipo tras el mantenimiento, inspeccionarlo para asegurarse de que el equipo no ha sido manipulado y de que funciona correctamente k) aplicar medidas para la eliminación segura o la reutilización del equipo (véase 7.14) si se determina que equipo debe ser eliminado.
R1 R256 R524 R2 R257 R525 R5 R260 R528 R18 R267 R535 R19 R268 R536 R22 R271 R539 R35 R284 R546 R36 R285 R547 R39 R286 R550 R52 R288 R557 R53 R294 R558 R56 R295 R561 R69 R296 R568 R70 R298 R569 R73 R304 R572 R86 R305 R579 R87 R306 R580 R90 R308 R583 R103 R314 R590 R104 R315 R591 R107 R316 R594 R114 R318 R601 R115 R324 R602 R118 R325 R605 R125 R326 R612 R126 R328 R613 R129 R354 R616 R136 R355 R629 R137 R358 R630 R140 R401 R633 R146 R402 R640 R147 R405 R641 R150 R418 R644 R156 R419 R651 R157 R422 R652 R160 R435 R655 R173 R436 R668 R174 R439 R669 R177 R446 R672 R190 R447 R679 R191 R450 R680 R194 R463 R683 R201 R464 R249 R202 R467 R514 R205 R474 R245 R212 R475 R238 R213 R478 R513 R216 R491 R235 R223 R492 R506 R224 R495 R503 R227 R502 R234 R246 R517	7.5 Control: Se debe diseñar e implementar la protección contra amenazas físicas y ambientales, tales como desastres naturales y otras amenazas físicas intencionales o no intencionales a la infraestructura.	Las evaluaciones de riesgos para identificar las consecuencias potenciales de las amenazas físicas y medioambientales deben realizarse antes de iniciar operaciones críticas en un emplazamiento físico, y a intervalos regulares. Debe obtenerse asesoramiento especializado sobre cómo gestionar los riesgos derivados de amenazas físicas y medioambientales como incendios, inundaciones, terremotos, explosiones, disturbios civiles, residuos tóxicos, emisiones medioambientales y otras formas de catástrofes naturales o provocadas por el hombre. formas de catástrofes naturales o provocadas por el ser humano. La ubicación física de los locales y su construcción deben tener en cuenta a) la topografía local, como la elevación adecuada, las masas de agua y las fallas tectónicas; b) las amenazas urbanas, como los lugares con un perfil alto para atraer disturbios políticos, actividad delictiva o atentados terroristas.

Riesgo	Control de la Norma	Estrategia
R11 R266 R545 R28 R277 R556 R45 R364 R567 R62 R411 R578 R79 R428 R589 R96 R445 R600 R113 R456 R611 R124 R473 R622 R135 R484 R639 R166 R501 R650 R183 R512 R661 R200 R523 R678 R211 R534 R689 R222 R696 R255 R233 R244	8.12 Control: Las medidas de prevención de fuga de datos se aplicarán a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible	La organización debe tener en cuenta lo siguiente para reducir el riesgo de fuga de datos: a) identificar y clasificar la información para protegerla contra fugas (por ejemplo, información personal, modelos de precios y diseños de productos); b) controlar los canales de fuga de datos (por ejemplo, correo electrónico, transferencias de archivos, dispositivos móviles y dispositivos de almacenamiento portátiles); c) actuar para evitar la fuga de información (por ejemplo, poner en cuarentena los correos electrónicos que contengan información sensible). Las herramientas de prevención de fuga de datos deben utilizarse para: a) identificar y controlar la información sensible en riesgo de divulgación no autorizada (por ejemplo, en datos no estructurados en el sistema de un usuario); b) detectar la divulgación de información sensible (por ejemplo, cuando la información se carga en servicios en la nube de terceros no fiables o se envía por correo electrónico); c) bloquear acciones del usuario o transmisiones de red que expongan información sensible (por ejemplo, impedir la copia de entradas de una base de datos en una hoja de cálculo).
R4 R289 R516 R21 R299 R527 R38 R309 R538 R55 R319 R549 R72 R329 R560 R89 R334 R571 R106 R342 R582 R117 R344 R593 R128 R352 R604 R139 R357 R615 R149 R371 R632 R159 R379 R643 R176 R381 R654 R193 R389 R671 R204 R391 R682 R215 R399 R690 R226 R404 R477 R237 R421 R494 R248 R438 R505 R259 R449 R270 R466	8.14 Control: Las instalaciones de procesamiento de información se implementarán con suficiente redundancia para cumplir con los requisitos de disponibilidad.	La organización debe identificar los requisitos para la disponibilidad de los servicios empresariales y los sistemas de información. La organización debe diseñar e implantar una arquitectura de sistemas con la redundancia adecuada para cumplir estos requisitos. La redundancia puede introducirse duplicando las instalaciones de procesamiento de información en parte o en su totalidad (es decir, componentes de repuesto o tener dos de cada cosa). La organización debe planificar y procedimientos para la activación de los componentes e instalaciones de procesamiento redundantes. Los procedimientos deben establecer si los componentes redundantes y las actividades de procesamiento están siempre o, en caso de emergencia, se activan automática o manualmente. Los componentes redundantes e instalaciones de tratamiento de la información redundantes deben garantizar el mismo nivel de seguridad que los primarios. Deben existir mecanismos que alerten a la organización de cualquier fallo en las instalaciones de procesamiento de la información, permitan ejecutar el procedimiento previsto y permitan mantener la disponibilidad mientras se reparan o sustituyen las instalaciones de procesamiento de la información. A la hora de implantar sistemas redundantes, la organización debe tener en cuenta lo siguiente: a) contratar a dos o más proveedores de instalaciones de red y de procesamiento de información crítica, como proveedores de servicios de Internet; b) utilizar redes redundantes c) utilizar dos centros de datos separados geográficamente con sistemas duplicados; d) el uso de fuentes de alimentación redundantes físicamente; e) el uso de múltiples instancias paralelas de componentes de software, con equilibrio de carga automático entre ellas (entre instancias en el mismo centro de datos o en centros

Riesgo	Control de la Norma	Estrategia
		de datos diferentes); f) tener componentes duplicados en los sistemas (por ejemplo, CPU, discos duros, memorias) o en las redes (por ejemplo, cortafuegos, enrutadores, conmutadores).
R15 R498 R32 R509 R49 R520 R66 R531 R83 R542 R100 R553 R110 R564 R121 R575 R170 R586 R187 R597 R197 R608 R208 R626 R219 R636 R230 R647 R241 R665 R252 R675 R263 R686 R281 R488 R368 R470 R415 R460 R432 R442	8.15 Control: Se producirán, almacenarán, protegerán y analizarán registros que registren actividades, excepciones, fallas y otros eventos relevantes	La organización debe determinar el propósito para el que se crean los registros, qué datos se recopilan y registran, y cualquier requisito específico de los registros para protegerlos y manejarlos. Esto debe documentarse en una política específica sobre registros. Los registros de eventos deben incluir para cada evento, según corresponda a) ID de usuario; b) actividades del sistema c) fechas, horas y detalles de los eventos relevantes (por ejemplo, inicio y cierre de sesión); d) identidad del dispositivo, identificador del sistema y ubicación; e) direcciones y protocolos de red. Deben tenerse en cuenta para el registro los siguientes eventos a) intentos de acceso al sistema aceptados y rechazados; b) intentos exitosos y rechazados de acceso a datos y otros recursos; c) cambios en la configuración del sistema d) uso de privilegios e) uso de programas de utilidad y aplicaciones f) archivos a los que se ha accedido y tipo de acceso, incluida la eliminación de archivos de datos importantes; g) alarmas emitidas por el sistema de control de acceso; h) activación y desactivación de sistemas de seguridad, como sistemas antivirus y de detección de intrusos; i) creación, modificación o supresión de identidades j) transacciones ejecutadas por los usuarios en las aplicaciones. En algunos casos, las aplicaciones son un servicio o producto proporcionado o gestionado por un tercero.
R343 R353 R380 R390 R400	8.16 Control: Las redes, los sistemas y las aplicaciones deberán ser monitoreados por comportamiento anómalo y se tomarán las acciones apropiadas para evaluar posibles incidentes de seguridad de la información.	El alcance y el nivel de la supervisión deben determinarse de acuerdo con los requisitos de la empresa y de la seguridad de la información y teniendo en cuenta las leyes y reglamentos pertinentes. Los registros de supervisión deben conservarse durante periodos definidos. Deberá considerarse la inclusión de los siguientes elementos en el sistema de supervisión: a) tráfico saliente y entrante de la red, del sistema y de las aplicaciones; b) acceso a sistemas, servidores, equipos de red, sistema de supervisión, aplicaciones críticas, etc.; c) archivos de configuración de red y de sistemas críticos o de nivel de administrador; d) registros de herramientas de seguridad [por ejemplo, antivirus, IDS, sistema de prevención de intrusiones (IPS), filtros web, cortafuegos, prevención de fuga de datos]; e) registros de eventos relativos a la actividad del sistema y de la red; f) comprobación de que el código que se está ejecutando está autorizado a ejecutarse en el sistema y que no ha sido manipulado (por ejemplo, mediante la recopilación para añadir código adicional no deseado); g) el uso de los recursos (por ejemplo, CPU, discos duros, memoria, ancho de banda) y su rendimiento.

Riesgo	Control de la Norma	Estrategia
		La organización debe establecer una línea de base del comportamiento normal y controlar las anomalías con respecto a esta línea de base. Al establecer una línea de base, debe tenerse en cuenta lo siguiente: a) revisión de la utilización de los sistemas en periodos normales y punta; b) la hora habitual de acceso, el lugar de acceso y la frecuencia de acceso de cada usuario o grupo de usuarios. El sistema de supervisión debe configurarse en función de la línea de base establecida para identificar comportamientos anómalos, como: a) terminación no planificada de procesos o aplicaciones; b) actividad típicamente asociada a malware o tráfico procedente de direcciones IP o dominios de red maliciosos conocidos (por ejemplo, los asociados a servidores de mando y control de botnets); c) características de ataque conocidas (por ejemplo, denegación de servicio y desbordamientos de búfer) d) comportamiento inusual del sistema (por ejemplo, registro de pulsaciones de teclas, inyección de procesos y desviaciones en el uso de protocolos estándar); e) cuellos de botella y sobrecargas (por ejemplo, colas en la red, niveles de latencia y fluctuación de la red); f) acceso no autorizado (real o intentado) a sistemas o información g) exploración no autorizada de aplicaciones, sistemas y redes empresariales h) intentos exitosos e infructuosos de acceder a recursos protegidos (por ejemplo, servidores DNS, portales web y sistemas de archivos); i) comportamiento inusual de usuarios y sistemas en relación con el comportamiento esperado.
R702	8.24 Control: Se deben definir e implementar reglas para el uso efectivo de la criptografía, incluida la gestión de claves criptográficas.	A la hora de utilizar criptografía, debe tenerse en cuenta lo siguiente a) la política específica sobre criptografía definida por la organización, incluidos los principios generales de protección de la información. Una política temática específica sobre el uso de la criptografía es necesaria para maximizar los beneficios y minimizar los riesgos del uso de técnicas criptográficas y evitar un uso inadecuado o incorrecto; b) identificar el nivel de protección requerido y la clasificación de la información y en consecuencia, establecer el tipo, la fuerza y la calidad de los algoritmos criptográficos necesarios. c) el uso de la criptografía para la protección de la información contenida en los dispositivos móviles de los usuarios o en los medios de almacenamiento y transmitida a través de las redes a dichos dispositivos o soportes de almacenamiento d) el enfoque de la gestión de claves, incluidos los métodos para tratar la generación y protección de claves criptográficas y la recuperación de la información cifrada en caso de pérdida, compromiso o dañadas; e) funciones y responsabilidades para: 1) la aplicación de las normas para el uso eficaz de la criptografía; 2) la gestión de claves, incluida la generación de claves (véase 8.24) f) las normas que deben adoptarse, así como los algoritmos criptográficos, la fuerza de cifrado, las soluciones criptográficas y prácticas de uso aprobadas o exigidas en la

Riesgo	Control de la Norma	Estrategia
		organización; g) el impacto del uso de información cifrada en los controles que se basan en la inspección de contenidos (por ejemplo, detección de malware o filtrado de contenidos).
R9 R26 R43 R60 R77 R94 R133 R144 R164 R181 R275 R291 R301 R311 R321 R331 R337 R347 R362 R374 R384 R394 R409 R426 R454 R482 R620 R659	8.32 Control: Los cambios en las instalaciones de procesamiento de información y los sistemas de información estarán sujetos a procedimientos de gestión de cambios.	La introducción de nuevos sistemas y de cambios importantes en los existentes debe seguir unas normas acordadas y un proceso formal de documentación, especificación, prueba, control de calidad y gestión de la aplicación. Deben establecerse responsabilidades y procedimientos de gestión para garantizar un control satisfactorio de todos los cambios. Los procedimientos de control de cambios deben documentarse y aplicarse para garantizar la confidencialidad, integridad y disponibilidad de la información en las instalaciones de tratamiento de la información y los sistemas de información, durante todo el ciclo de vida de desarrollo del sistema, desde la fase inicial hasta la fase final. Siempre que sea posible, deben integrarse los procedimientos de control de cambios para la infraestructura y el software de TIC. Los procedimientos de control de cambios deben incluir a) planificación y evaluación del impacto potencial de los cambios teniendo en cuenta todas las dependencias; b) autorización de los cambios c) la comunicación de los cambios a las partes interesadas pertinentes. d) pruebas y aceptación de las pruebas de los cambios (véase 8.29); e) aplicación de los cambios, incluidos los planes de despliegue f) consideraciones de emergencia y contingencia, incluidos los procedimientos de emergencia; g) mantenimiento de registros de los cambios que incluyan todo lo anterior; h) garantizar que la documentación operativa (véase 5.37) y los procedimientos de usuario se modifiquen según sea necesario para seguir siendo adecuados; i) garantizar que los planes de continuidad de las TIC y los procedimientos de respuesta y recuperación (véase 5.30) se modifican según sea necesario para seguir siendo apropiados.
R7 R293 R574 R14 R303 R585 R24 R313 R596 R31 R323 R607 R41 R333 R618 R48 R339 R625 R58 R340 R635 R65 R341 R646 R75 R349 R657 R82 R350 R664 R92 R351 R674	8.6 Control: El uso de los recursos se controlará y ajustará de acuerdo con los requisitos de capacidad actuales y previstos.	Deben determinarse las necesidades de capacidad de las instalaciones de procesamiento de la información, los recursos humanos, las oficinas y otras instalaciones, teniendo en cuenta la criticidad empresarial de los sistemas y procesos en cuestión. El ajuste y la supervisión del sistema deben aplicarse para garantizar y, en caso necesario, mejorar la disponibilidad y eficiencia de los sistemas. La organización debe realizar pruebas de estrés de los sistemas y servicios para confirmar que se dispone de suficiente capacidad del sistema para satisfacer los requisitos de rendimiento máximo. Las proyecciones de las necesidades futuras de capacidad deben tener en cuenta las nuevas necesidades de la empresa y del sistema, así como las tendencias actuales y previstas en el mercado. y previstas en las capacidades de procesamiento de la información de la organización. Debe prestarse especial atención a los recursos con plazos de adquisición largos o costes elevados. Por lo tanto, los gestores y los propietarios de servicios o

Riesgo	Control de la Norma	Estrategia
R99 R360 R685 R109 R367 R692 R120 R376 R487 R131 R377 R497 R142 R378 R508 R152 R386 R519 R154 R387 R530 R162 R388 R541 R169 R396 R552 R179 R397 R563 R186 R398 R280 R196 R407 R480 R207 R414 R273 R218 R424 R469 R229 R431 R262 R240 R441 R459 R251 R452		productos deben supervisar la utilización de los recursos clave del sistema. Los gestores deben utilizar la información sobre capacidad para identificar y evitar posibles limitaciones de recursos y dependencia de personal clave que puedan suponer una amenaza para la seguridad del sistema o los servicios, y planificar las medidas oportunas. Se puede conseguir una capacidad suficiente aumentando la capacidad o reduciendo la demanda. Para aumentar la capacidad debe considerarse lo siguiente a) contratar nuevo personal b) obtención de nuevas instalaciones o espacio c) adquirir sistemas de procesamiento, memoria y almacenamiento más potentes; d) hacer uso de la computación en nube, que tiene características inherentes que abordan directamente los problemas de capacidad. La computación en nube tiene elasticidad y escalabilidad que permiten ampliar y reducir rápidamente los recursos disponibles para determinadas aplicaciones y servicios. Para reducir la demanda de recursos de la organización, debe tenerse en cuenta lo siguiente: a) eliminación de datos obsoletos (espacio en disco) b) eliminación de registros impresos que hayan cumplido su periodo de conservación (liberar espacio en las estanterías); c) desmantelamiento de aplicaciones, sistemas, bases de datos o entornos; d) optimización de procesos y programaciones por lotes e) optimización del código de las aplicaciones o de las consultas a las bases de datos f) denegación o restricción de ancho de banda para servicios que consuman recursos si no son críticos (por ejemplo, streaming de vídeo).
R10 R27 R44 R61 R78 R95 R112 R123		La protección contra los programas maliciosos debe basarse en software de detección y reparación de programas maliciosos, concienciación sobre la seguridad de la información, acceso adecuado al sistema y controles de gestión de cambios. El uso de software no suele ser suficiente. Deben tenerse en cuenta las siguientes orientaciones: a) aplicar normas y controles que impidan o detecten el uso de software no autorizado [por ejemplo lista de aplicaciones permitidas (es decir, utilizar una lista que proporcione las aplicaciones permitidas)] (véanse 8.19 y 8.32); b) aplicar controles que impidan o detecten el uso de sitios web conocidos o sospechosos de ser maliciosos (por ejemplo, listas de bloqueo); c) reducir las vulnerabilidades que pueden ser explotadas por programas maliciosos [por ejemplo, mediante la gestión técnica de vulnerabilidades (véanse los puntos 8.8 y 8.19)]; d) realizar una validación automatizada periódica del contenido de software y datos de los sistemas, especialmente en el caso de los sistemas que soportan procesos empresariales críticos; investigar la presencia de cualquier archivo no aprobado o modificación no autorizada; e) establecer medidas de protección contra los riesgos asociados a la obtención de archivos y programas informáticos desde o a través de redes externas o en cualquier otro soporte f) instalar y actualizar periódicamente software de detección y reparación de malware para escanear ordenadores y medios de almacenamiento electrónico. Realización de

Riesgo	Control de la Norma	Estrategia
R134 R145 R165 R182 R199 R210 R221 R232 R243 R254 R265 R276 R363 R410 R427 R444 R455 R472 R483 R500 R511 R522 R533 R544 R555 R566 R577 R588 R599 R610 R621 R638 R649 R660 R677 R688 R695	8.7 Control: La protección contra el malware se implementará y respaldará mediante la conciencia adecuada del usuario.	análisis periódicos que incluyan: 1) escaneo de cualquier dato recibido a través de redes o mediante cualquier forma de medio de almacenamiento electrónico, en busca de malware antes de su uso; 2) escanear los archivos adjuntos y las descargas de correo electrónico y mensajería instantánea en busca de programas maliciosos antes de utilizarlos. Realizar este escaneado en diferentes lugares (por ejemplo, en servidores de correo electrónico, ordenadores de sobremesa) y al entrar en la red de la organización; 3) escanear las páginas web en busca de malware cuando se acceda a ellas; g) determinar la ubicación y configuración de las herramientas de detección y reparación de malware en función de los resultados de la evaluación de riesgos y teniendo en cuenta 1) los principios de defensa en profundidad, donde serían más eficaces. Por ejemplo, esto puede conducir a la detección de programas maliciosos en una pasarela de red (en varios protocolos de aplicación como el correo electrónico, la transferencia de archivos y la web), así como en dispositivos y servidores de punto final del usuario; 2) las técnicas evasivas de los atacantes (por ejemplo, el uso de archivos cifrados) para transmitir programas maliciosos o el uso de protocolos de cifrado para transmitir programas maliciosos; h) velar por la protección contra la introducción de programas maliciosos durante los procedimientos de mantenimiento y emergencia, que pueden eludir los controles normales contra los programas maliciosos; i) aplicar un proceso para autorizar la desactivación temporal o permanente de algunas o todas las medidas contra programas maliciosos, que incluya autoridades de aprobación de excepciones, justificación documentada y fecha de revisión. Esto puede ser necesario cuando la protección contra el malware cause interrupciones en las operaciones normales; j) preparar planes adecuados de continuidad de la actividad para recuperarse de los ataques de programas maliciosos, incluidas todas las copias de seguridad de datos y programas informáticos necesarias (incluidas las copias de seguridad en línea y fuera de línea) y las medidas de recuperación (véase 8.13); k) aislar los entornos en los que puedan producirse consecuencias catastróficas; l) definir procedimientos y responsabilidades para tratar la protección contra programas maliciosos en los sistemas, incluida la formación sobre su uso, la notificación y la recuperación en caso de ataques de programas maliciosos; m) sensibilizar o formar (véase 6.3) a todos los usuarios sobre cómo identificar y potencialmente mitigar la recepción, el envío o la instalación de correos electrónicos, archivos o programas infectados con programas maliciosos [la información recogida puede utilizarse para garantizar que la sensibilización y la formación se mantienen actualizadas]; n) aplicar procedimientos para recopilar periódicamente información sobre nuevos programas maliciosos, como suscribirse a listas de correo o consultar sitios web pertinentes; o) verificar que la información relativa a los programas maliciosos, como los boletines de alerta, procede de fuentes cualificadas y acreditadas (por ejemplo, sitios de Internet

Riesgo	Control de la Norma	Estrategia
		fiables o proveedores de programas informáticos de detección de programas maliciosos) y es exacta e informativa.
R13 R17 R30 R34 R47 R51 R64 R68 R81 R85 R98 R102 R168 R172 R185 R189 R279 R283 R292 R302 R312 R322 R332 R366 R370 R413 R417 R430 R434 R458 R462 R486 R490 R624 R628 R663 R667	8.8 Control: Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se debe evaluar la exposición de la organización a tales vulnerabilidades y se deben tomar las medidas apropiadas.	Identificación de vulnerabilidades técnicas La organización debe disponer de un inventario preciso de los activos (véanse los puntos 5.9 a 5.14) como requisito previo para una gestión eficaz de las vulnerabilidades técnicas; el inventario debe incluir el proveedor del software, el nombre del software, los números de versión, el estado actual de despliegue (por ejemplo, qué software está instalado en qué sistemas) y la(s) persona(s) responsable(s). sistemas) y la(s) persona(s) de la organización responsable(s) del software. Para identificar las vulnerabilidades técnicas, la organización debe considerar: a) definir y establecer las funciones y responsabilidades asociadas a la gestión de las vulnerabilidades técnicas, incluida la supervisión de la vulnerabilidad, la evaluación del riesgo de vulnerabilidad, la actualización, el seguimiento de los activos y cualquier responsabilidad de coordinación necesaria; b) para el software y otras tecnologías (basándose en la lista del inventario de activos, véase 5.9), identificar los recursos de información que se utilizarán para identificar las vulnerabilidades técnicas pertinentes y mantener el conocimiento sobre ellas. Actualizar la lista de recursos de información en función de los cambios en el inventario o cuando se encuentren otros recursos nuevos o útiles; c) Exigir a los proveedores de sistemas de información (incluidos sus componentes) que garanticen la notificación, el tratamiento y la divulgación de las vulnerabilidades, incluidos los requisitos de los contratos aplicables (véase 5.20); d) utilizar herramientas de exploración de vulnerabilidades adecuadas a las tecnologías en uso para identificar vulnerabilidades y verificar si el parcheado de vulnerabilidades se ha realizado con éxito; e) realizar pruebas de penetración o evaluaciones de vulnerabilidad planificadas, documentadas y repetibles por personas competentes y autorizadas para apoyar la identificación de vulnerabilidades. Extremar las precauciones, ya que tales actividades pueden comprometer la seguridad del sistema; f) rastrear el uso de bibliotecas y código fuente de terceros en busca de vulnerabilidades. Esto debería incluirse en la codificación segura (véase 8.28). La organización debe desarrollar procedimientos y capacidades para: a) detectar la existencia de vulnerabilidades en sus productos y servicios, incluyendo cualquier componente externo utilizado en los mismos; b) recibir informes sobre vulnerabilidades de fuentes internas o externas. Evaluación de las vulnerabilidades técnicas Para evaluar las vulnerabilidades técnicas detectadas, deben tenerse en cuenta las siguientes orientaciones: a) analizar y verificar los informes para determinar qué actividad de respuesta y reparación es necesaria; b) una vez identificada una posible vulnerabilidad técnica, identificar los riesgos asociados y las acciones que deben emprenderse. Dichas acciones pueden implicar la actualización de los sistemas vulnerables o la aplicación de

Riesgo	Control de la Norma	Estrategia
		otros controles. Adopción de medidas adecuadas para hacer frente a las vulnerabilidades técnicas: Debe implantarse un proceso de gestión de actualizaciones de software para garantizar que se instalan los parches aprobados y las actualizaciones de aplicaciones más recientes para todo el software autorizado. Si es necesario realizar cambios, debe conservarse el software original y aplicar los cambios a una copia designada. Todas las modificaciones deben probarse y documentarse por completo, de modo que puedan volver a aplicarse, en caso necesario, a futuras actualizaciones del software. En caso necesario, las modificaciones deberán ser probadas y validadas por un organismo de evaluación independiente. Para hacer frente a las vulnerabilidades técnicas, deben tenerse en cuenta las siguientes orientaciones a) tomar medidas adecuadas y oportunas en respuesta a la identificación de vulnerabilidades técnicas potenciales; definir un calendario para reaccionar ante las notificaciones de vulnerabilidades técnicas potencialmente relevantes; b) en función de la urgencia con que deba abordarse una vulnerabilidad técnica, llevar a cabo la acción de acuerdo con los controles relacionados con la gestión de cambios (véase 8.32) o siguiendo los procedimientos de respuesta a incidentes de seguridad de la información (véase 5.26); c) utilizar únicamente actualizaciones de fuentes legítimas (que pueden ser internas o externas a la organización); d) probar y evaluar las actualizaciones antes de instalarlas para asegurarse de que son eficaces y no provocan efectos secundarios que no puedan tolerarse [es decir, si hay una actualización disponible, evaluar los riesgos asociados a la instalación de la actualización (los riesgos que plantea la vulnerabilidad deben compararse con el riesgo de instalar la actualización)]; e) abordar primero los sistemas de alto riesgo f) desarrollar medidas correctoras (normalmente actualizaciones o parches de software); g) realizar pruebas para confirmar si la corrección o mitigación es eficaz; h) proporcionar mecanismos para verificar la autenticidad de la reparación; i) si no hay ninguna actualización disponible o la actualización no puede instalarse, considerar otros controles, tales como 1) aplicar cualquier solución alternativa sugerida por el proveedor del software u otras fuentes pertinentes; 2) desactivar servicios o capacidades relacionados con la vulnerabilidad; 3) adaptar o añadir controles de acceso (por ejemplo, cortafuegos) en las fronteras de la red (véanse los puntos 8.20 a 8.22); 4) blindar los sistemas, dispositivos o aplicaciones vulnerables frente a los ataques mediante el despliegue de filtros de tráfico adecuados (lo que a veces se denomina parcheado virtual); 5) aumentar la vigilancia para detectar ataques reales 6) aumentar la concienciación sobre la vulnerabilidad.