1. OBJETIVO

a) Asegurar la capacidad necesaria de los servicios de procesamiento de información, los recursos humanos, las oficinas y otros servicios.
b) Asegurar que la información y otros activos asociados estén protegidos contra malware.
c) Evitar la explotación de vulnerabilidades técnicas.
d) Asegurar que el hardware, el software, los servicios y las redes funcionen correctamente con la configuración de seguridad y privacidad requerida y la configuración no se vea alterada por cambios no autorizados o incorrectos.
e) Evitar la exposición innecesaria de información confidencial y cumplir con los requisitos legales, reglamentarios y contractuales para la eliminación de información.
f) Limitar la exposición de datos sensibles incluida la Información de Identificación Personal (IIP) y cumplir con los requisitos legales, estatutarios, reglamentarios y contractuales.
g) Detectar y prevenir la divulgación y extracción no autorizada de información por parte de individuos o sistemas.
h) Registrar eventos, generar pruebas,
i) Asegurar la integridad de la información de registro, evitar el acceso no autorizado, identificar eventos de seguridad y/o privacidad de la información que pueden dar lugar a un incidente de seguridad y/o privacidad de la información y respaldar las investigaciones.
j) Detectar comportamientos anómalos y posibles incidentes de seguridad y privacidad de la información.
k) Permitir la correlación y el análisis de los eventos relacionados con la seguridad, privacidad de la información y otros datos registrados y apoyar las investigaciones sobre incidentes de seguridad de la información.
l) Asegurar que el uso de programas de utilidad no perjudique los controles del sistema y de las aplicaciones para la seguridad y privacidad de la información.
m) Asegurar la integridad de los sistemas operativos y evitar la explotación de las vulnerabilidades técnicas.
n) Proteger los sistemas contra el peligro de malware y para evitar el acceso a recursos no autorizador de la web.
o) Minimizar el impacto de las auditorías y otras actividades de garantía en los sistemas operativos y los procesos de la Institución.

2. ALCANCE

Las presentes directrices aplican a todos los funcionarios administrativos, docentes, estudiantes, judicantes, pasantes, contratistas y/o terceros de la Universidad Surcolombiana.

3. DEFINICIONES

Entidad: puede representar a un usuario humano, así como a un elemento técnico o lógico (por ejemplo, una máquina, un dispositivo o un servicio)

Información de Identificación Personal (IIP): cualquier dato que pueda utilizarse para identificar a alguien. Toda la información que se relaciona directa o indirectamente con una persona se considera IIP

Malware: cualquier tipo de software malicioso diseñado para dañar o explotar cualquier dispositivo, servicio o red programable.

4. MARCO DE REFERENCIA

La gestión de riesgos y oportunidades en la Universidad Surcolombiana considera para su labor, los lineamientos definidos en las directrices y políticas institucionales, además de las consideraciones definidas en:

- La norma ISO 31000:2018– Gestión del riesgo. Principios y directrices.
- La norma ISO IEC 27005:2022 – Gestión de riesgos para la seguridad de la información.
- Los lineamientos definidos en los documentos del Sistema de Gestión de Seguridad y Privacidad de la Información.
- Los requisitos aplicables a la gestión del riesgo, detallados en el estándar ISO IEC 27001:2022 y la ISO IEC 27701:2025
- Código de Práctica para Controles de Seguridad de la Información - GTC ISO IEC 27002:2022 Tecnología de la Información. Técnicas de Seguridad.
- Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías y Sistemas de Información.

- Guía de Administración de riesgos y el diseño de controles en entidades públicas
- CONPES de Seguridad Digital (CONPES 3854 de 2016 y actualizaciones)
- Modelo de Seguridad y Privacidad de la Información – MSPI (MinTIC)
- Política de Gobierno Digital (Decreto 1078 de 2015 y actualizaciones)
- Modelo Integrado de Planeación y Gestión – MIPG (DAFP)
- FURAG (Formulario Único de Reporte de Avance de la Gestión)
- Ley 1581 de 2012 y Decreto 1377 de 2013
- Lineamientos y guías de la Superintendencia de Industria y Comercio.

5. GENERALIDADES

Estas directrices son la declaración general que establece la Universidad para los controles tecnológicos, con base en los siguientes controles de acuerdo a las normas:

ISO/IEC 27001:2022

A.8.6 Gestión de capacidad
A.8.7 Protección contra malware
A.8.8 Gestión de las vulnerabilidades técnicas
A.8.9 Gestión de la configuración
A.8.10 Eliminación de información
A.8.11 Enmascaramiento de datos
A.8.12 Prevención de la fuga de datos
A.8.15 Registros
A.8.16 Actividades de monitoreo
A.8.17 Sincronización del reloj
A.8.18 Uso de programas de utilidad privilegiados
A.8.19 Instalación de software en sistemas operativos
A.8.23 Filtrado web
A.8.34 Protección de los sistemas de información durante las pruebas de auditoría

ISO/IEC 27701:2025

A.3.25 Registro de actividades

6. DIRECTRICES

6.1. GESTIÓN DE CAPACIDAD

La Universidad debe determinar las necesidades de capacidad para las instalaciones de procesamiento de información, los recursos humanos, las oficinas y otras instalaciones, tomando en consideración los servicios misionales y teniendo siempre en cuenta la disponibilidad y eficacia de los sistemas de información.

El Centro de Información, Tecnología y Control Documental (CITCD) debe realizar pruebas de esfuerzo de los sistemas y servicios para confirmar que hay suficiente capacidad tecnológica para satisfacer los requisitos de rendimiento máximo.

En las proyecciones de los futuros requisitos de capacidad deben tener en cuenta los nuevos requisitos de la Universidad y de sus sistemas, así como las tendencias actuales.

Se deben tomar en consideración las siguientes directrices para aumentar la capacidad:

a) contratación de nuevo personal;

b) obtención de nuevas instalaciones o espacio;

c) adquisición de sistemas de procesamiento, memoria y almacenamiento más potentes;

d) uso de computación en la nube (*cloud computing*)

Para reducir la demanda de los recursos de la organización, se debe tener en cuenta lo siguiente:

a) eliminación de datos obsoletos (espacio en disco);

b) eliminación de registros impresos que hayan cumplido su período de retención (liberar espacio para estanterías);

c) dar de baja aplicaciones, sistemas, bases de datos o entornos;

d) optimización de procesos por lotes y programaciones;

e) optimización del código de aplicación o de las consultas a la base de datos;

f) rechazo o restricción del ancho de banda para servicios que consumen recursos si no son críticos (por ejemplo, transmisión de video).

Se debe considerar un plan de gestión de la capacidad para los sistemas de misión crítica.

6.2. PROTECCIÓN CONTRA MALWARE

La protección contra el malware debe basarse en software de detección y reparación de malware, conocimiento de la seguridad de la información, acceso adecuado al sistema y controles de gestión de cambios.

Se debe tomar en consideración las siguientes directrices:

a) implementar reglas y controles que impidan o detecten el uso de software no autorizado

b) implementar controles que impidan o detecten el uso de sitios web maliciosos conocidos o sospechosos; (listas de bloqueo)

c) reducir las vulnerabilidades que pueden ser explotadas por malware

d) realizar una validación automatizada regular del software y del contenido de datos de los sistemas, especialmente para los sistemas que soportan procesos críticos de la Institución; verificando la presencia de archivos no aprobados o modificaciones no autorizadas; software ESET Endpoint Antivirus, herramienta de Gestión de Activos de IT INVGATE.

e) establecer medidas de protección contra los riesgos asociados a la obtención de archivos y software ya sea desde o a través de redes externas o en cualquier otro medio;

f) instalación y actualización periódica de software de detección y reparación

de malware para analizar computadores y medios de almacenamiento electrónicos, que incluyan la realización de exploraciones regulares así:

1) cualquier dato recibido a través de redes o a través de cualquier medio de almacenamiento electrónico;

2) archivos adjuntos y descargas de correo electrónico y mensajería instantánea

3) páginas web

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

h) cuidar de la protección contra la introducción de malware durante el mantenimiento y los procedimientos de emergencia, que pueden eludir los controles normales contra el malware;

i) la implementación de un proceso para autorizar temporalmente o permanentemente la desactivación de algunas o todas las medidas contra el malware, incluidas las autoridades de aprobación de excepciones, la justificación documentada y la fecha de revisión. Esto puede ser necesario cuando la protección contra el malware provoca interrupciones en las operaciones normales;

j) preparar planes de continuidad del negocio adecuados para la recuperación de ataques de malware, incluidos todos los datos y copias de seguridad de software necesarios y las medidas de recuperación

k) aislamiento de entornos en los que pueden producirse consecuencias catastróficas;

l) definir procedimientos y responsabilidades para tratar la protección contra el malware en los sistemas, ver AP-TIC-PR-06 SOPORTE TÉCNICO DE EQUIPOS INFORMÁTICOS Y PUNTOS DE RED

m) Proporcionar conocimientos o formación a todos los usuarios sobre cómo

identificar y mitigar potencialmente la recepción, el envío o la instalación de correos electrónicos, archivos o programas infectados por malware

n) implementar procedimientos para recopilar periódicamente información sobre nuevos programas maliciosos, como la suscripción a listas de correo o la revisión de sitios web relevantes;

o) verificar que la información relacionada con el malware, como los boletines de advertencia, proveniente de fuentes calificadas y fiables. ver ES-GSPI-DA-03 GUIA FUENTES DE INFORMACIÓN DE AMENAZAS SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, ES-GSPI-DA-04 GUIA DE INTELIGENCIA DE AMENAZAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

6.3. GESTIÓN DE LAS VULNERABILIDADES TÉCNICAS

6.3.1 Identificación de vulnerabilidades técnicas

La Universidad debe tener un inventario de información y otros activos asociados, preciso como requisito previo para una gestión eficaz de la vulnerabilidad técnica; el inventario debe incluir el proveedor del software, el nombre del software, los números de versión, el estado actual de la implementación y la persona o personas dentro de la Institución, responsable del software.

Para identificar vulnerabilidades técnicas, se debe:

a) definir y establecer las funciones y responsabilidades asociadas con la gestión técnica de la vulnerabilidad, incluida la supervisión y la evaluación del riesgo de la misma, la actualización, el seguimiento de los activos de información y las responsabilidades de coordinación necesarias;

b) Mantener actualizado el inventario de activos y otros activos de información

c) exigir a los proveedores del sistema de información que garanticen la notificación, el tratamiento y la divulgación de vulnerabilidades, incluidos los requisitos de los contratos aplicables;

d) utilizar herramientas de análisis de vulnerabilidades adecuadas para las tecnologías en uso con el fin de identificar vulnerabilidades y comprobar si la aplicación de parches de vulnerabilidades se ha realizado correctamente;

e) realizar pruebas de penetración o evaluación de vulnerabilidad planificadas, documentadas y repetibles por parte de personas competentes y autorizadas para apoyar la identificación de vulnerabilidades.

f) realizar seguimiento del uso de bibliotecas de terceros y del código fuente en busca de vulnerabilidades. Esto debería ser incluido en la codificación segura.

La Universidad debe desarrollar procedimientos y capacidades para:

a) detectar la existencia de vulnerabilidades en sus productos y servicios, incluido cualquier componente externo utilizado en ellos;

b) recibir informes de vulnerabilidad de fuentes internas o externas.

6.3.2 Evaluación de vulnerabilidades técnicas

Para evaluar las vulnerabilidades técnicas identificadas, se debe tener en cuenta:

a) analizar y verificar los informes para determinar qué respuesta y actividad de corrección son necesarias;

b) una vez identificada una posible vulnerabilidad técnica, se identifican los riesgos asociados y las medidas que se deberían tomar. Estas acciones pueden implicar la actualización de sistemas vulnerables o la aplicación de otros controles.

6.3.3 Tomar las medidas adecuadas para abordar las vulnerabilidades técnicas.

El CITCD debe implementar un proceso de gestión de actualizaciones de software para asegurar que se instalan los parches y actualizaciones de

aplicaciones aprobados más actualizados para todo el software autorizado. Si es necesario realizar cambios, se debe conservar el software original y aplicar los cambios a una copia designada. Todos los cambios deben probarse y documentarse por completo, de modo que se puedan volver a aplicar, si es necesario, a futuras actualizaciones de software.

Para abordar vulnerabilidades técnicas se debe tener en cuenta:

a) adoptar medidas apropiadas y oportunas en respuesta a la identificación de posibles vulnerabilidades técnicas; definir un calendario para reaccionar a las notificaciones de vulnerabilidades técnicas potencialmente relevantes, a través de un plan de tratamiento de las mismas;

b) dependiendo de la urgencia con que se deba abordar una vulnerabilidad técnica, llevar a cabo la acción de acuerdo con los controles relacionados con la gestión de cambios o siguiendo los procedimientos de respuesta a incidentes de seguridad y/o privacidad de la información;

c) solo utilizar 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 efectivas y no producen efectos secundarios que no se pueden tolerar;

e) abordar primero los sistemas de alto riesgo;

f) desarrollar soluciones, actualizaciones de software o parches;

g) realizar pruebas para confirmar si la remediación o mitigación es efectiva;

h) proporcionar mecanismos para verificar la autenticidad de la corrección;

i) si no hay ninguna actualización disponible o la actualización no se puede instalar, se debe tomar en consideración controles como:

   1) aplicar cualquier solución sugerida por el proveedor del software u otras fuentes relevantes;

2) desactivar servicios o capacidades relacionados con la vulnerabilidad;

3) adaptar o añadir controles de acceso, como los firewalls en los límites de la red

4) protección de sistemas, dispositivos o aplicaciones vulnerables frente a ataques mediante la implementación de filtros de tráfico adecuados

5) aumentar la supervisión para detectar ataques reales;

6) sensibilización sobre la vulnerabilidad.

La ejecución de este control podrá ser realizada por personal interno de la Universidad o por un proveedor especializado que tenga la competencia requerida para esta actividad.

6.4. GESTIÓN DE LA CONFIGURACIÓN

El CITCD debe definir e implementar procesos y herramientas para aplicar las configuraciones definidas (incluidas las configuraciones de seguridad y privacidad) para hardware, software, servicios y redes, para sistemas recién instalados y para sistemas operativos a lo largo de su vida útil.

6.4.1 Plantillas estándar

Se debe definir plantillas estándar para la configuración segura de hardware, software, servicios y redes, teniendo en cuenta lo siguiente:

a) minimizar el número de identidades con derechos de acceso a nivel de administrador o con privilegios;

b) deshabilitar identidades innecesarias, no utilizadas o inseguras;

c) deshabilitar o restringir funciones y servicios innecesarios;

d) restringir el acceso a potentes programas de utilidad y a la configuración de parámetros de host;

e) sincronización de relojes;

f) cambiar la información de autenticación predeterminada del proveedor, como las contraseñas predeterminadas, inmediatamente después de la instalación y revisar otros parámetros importantes relacionados con la seguridad predeterminada;

g) invocar las funciones de tiempo de espera que desconectan automáticamente los dispositivos informáticos después de un período predeterminado de inactividad;

h) verificar que se han cumplido los requisitos de licencia

Las plantillas deben revisarse periódicamente y actualizarse cuando sea necesario abordar nuevas amenazas o vulnerabilidades o cuando se introduzcan nuevas versiones de software o hardware. PLANTILLAS DE DESARROLLO DE SOFTWARE.

6.4.2 Gestión de configuraciones

Se debe registrar las configuraciones establecidas de hardware, software, servicios y redes y mantener un registro de todos los cambios de configuración. Estos registros deben almacenarse de forma segura.

Los cambios en las configuraciones deben seguir el proceso de administración de cambios. Los registros de configuración pueden contener, según corresponda:

a) información actualizada del propietario o punto de contacto del activo;

b) fecha del último cambio de configuración;

c) versión de la plantilla de configuración;

d) relación con las configuraciones de otros .

6.4.3 Configuraciones de monitoreo

Las configuraciones deben monitorearse con un conjunto completo de herramientas de administración del sistema (por ejemplo, servicios de mantenimiento, soporte remoto, herramientas de administración de la Institución, software de copia de seguridad y restauración) y deben revisarse periódicamente para verificar la configuración, evaluar la intensidad de la contraseña y evaluar las actividades realizadas. Consolas de VMWare, Hyper-V, InvGate

6.5. ELIMINACIÓN DE INFORMACIÓN

La información confidencial no debe conservarse durante más tiempo del necesario para reducir el riesgo de divulgación. Al eliminar información sobre sistemas, aplicaciones y servicios, se debe tener en cuenta lo siguiente:

a) selección de un método de borrado (por ejemplo, sobreescritura electrónica o borrado cifrado) de acuerdo con los requisitos de la Universidad, y tomando en consideración las leyes y reglamentos pertinentes;

b) Registro de los resultados de la eliminación como prueba;

c) cuando se utilicen proveedores de servicios de eliminación de información, obtener de ellos pruebas de la eliminación de dicha información.

d) cuando terceros almacenen la información de la Universidad en su nombre, la Universidad debe considerar la inclusión de requisitos sobre la eliminación de información en los acuerdos de terceros para aplicarla durante y al terminar dichos servicios.

Métodos de eliminación

De conformidad con la directriz temática específica de la organización sobre la retención de datos y tomando en consideración la legislación y los reglamentos pertinentes, la información confidencial debería eliminarse cuando ya no sea necesaria mediante:

a) Configuración de sistemas para destruir información de forma segura

cuando ya no sea necesaria

b) eliminación de versiones obsoletas, copias y archivos temporales dondequiera que se encuentren;

c) uso de software de eliminación seguro aprobado para eliminar información de forma permanente para asegurar que la información no se pueda recuperar mediante herramientas forenses o de recuperación especializada;

d) uso de proveedores autorizados y certificados de servicios de eliminación segura;

e) uso de mecanismos de eliminación adecuados para el tipo de medio de almacenamiento que se va a desechar

Cuando se utilizan servicios en la nube, la Universidad debe comprobar si el método de eliminación proporcionado por el proveedor de servicios en la nube es aceptable y, en caso afirmativo, la Universidad debe utilizarlo o solicitar que el proveedor de servicios en la nube elimine la información. Estos procesos de eliminación se deben automatizar de acuerdo con las directrices específicas del tema, cuando estén disponibles y sean aplicables.

Para evitar la exposición accidental de información confidencial cuando el equipo se regresa a los proveedores, la información confidencial debería protegerse eliminando almacenamientos auxiliares y la memoria antes de que el equipo salga de las instalaciones de la Universidad.

Tomando en consideración que la eliminación segura de algunos dispositivos solo se puede lograr mediante la destrucción o el uso de las funciones integradas en estos, (por ejemplo “restaurar ajustes de fábrica”), la organización debe elegir el método apropiado de acuerdo con la clasificación de la información que manejan dichos dispositivos.

6.6. ENMASCARAMIENTO DE DATOS

La Universidad debe utilizar técnicas de enmascaramiento, pseudoanonimización o anonimización para la protección de los datos sensibles e información

confidencial.

Entre las técnicas adicionales para el enmascaramiento de datos se incluyen:

a) cifrado;
b) anular o eliminar caracteres;
c) números y fechas variables;
d) sustitución (cambiar un valor por otro para ocultar datos confidenciales);
e) reemplazar valores con su hash.

Al implementar técnicas de enmascaramiento de datos, se debería tener en cuenta lo siguiente:

a) no conceder a todos los usuarios acceso a todos los datos, por lo tanto, diseñar consultas y máscaras para mostrar solo los datos mínimos necesarios para el usuario;

b) diseñar e implementar un mecanismo de visualización de datos dependiendo de los roles que le hayan sido asignados a los usuarios, esto en los casos en los que algunos datos no deban ser visibles al usuario para algunos registros de un conjunto de datos;

c) cualquier requisito legal o reglamentario vigente

Al utilizar el enmascaramiento, la pseudoanonimización o la anonimización de los datos debe tenerse en cuenta lo siguiente:

- nivel de intensidad del enmascaramiento de datos, pseudoanonimización o anonimización según el uso de los datos procesados;
- controles de acceso a los datos procesados;
- acuerdos o restricciones sobre el uso de los datos procesados;
- la imposibilidad de cotejar los datos procesados con otra información para identificar al titular de la IIP;
- realizar un seguimiento de la provisión y recepción de los datos procesados.

6.7. PREVENCIÓN DE LA FUGA DE DATOS

La Universidad debe considerar los siguientes aspectos para reducir el riesgo de fuga de datos:

a) identificar y clasificar información

b) supervisar los canales de fuga de datos (correo electrónico, transferencias de archivos, dispositivos móviles y dispositivos de almacenamiento portátiles);

al igual debe utilizar herramientas de prevención de fugas de datos para:

a) identificar y supervisar la información confidencial en riesgo de divulgación no autorizada;

b) detectar la divulgación de información confidencial

c) bloquear las acciones de los usuarios o las transmisiones de red que exponen información confidencial

Cuando se realiza una copia de seguridad de los datos, se debe tener cuidado para asegurar la protección de la información confidencial mediante medidas como el cifrado, el control de acceso y la protección física de los medios de almacenamiento que contienen la copia de seguridad.

6.8. REGISTROS

La Universidad debe determinar el propósito para el que se crean los registros, los datos que se recopilan y registran y los requisitos específicos de los mismos para protegerlos y gestionarlos

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 de red y protocolos.

Los siguientes eventos deberían ser considerados para el registro:

a) intentos de acceso al sistema exitosos y rechazados;

b) datos correctos y rechazados y otros intentos de acceso a recursos;

c) cambios en la configuración del sistema;

d) uso de privilegios;

e) uso de programas y aplicaciones de utilidad;

f) los archivos a los que se accede y el tipo de acceso, incluida la eliminación de archivos de datos importantes;

g) alarmas generadas por el sistema de control de acceso;

h) activación y desactivación de sistemas de seguridad, como sistemas antivirus y sistemas de detección de intrusiones;

i) creación, modificación o eliminación de identidades;

j) transacciones ejecutadas por usuarios en aplicaciones. En algunos casos, las aplicaciones son un servicio o producto proporcionado o ejecutado por un tercero.

Es importante que todos los sistemas tengan orígenes de tiempo sincronizados ya que esto permite la correlación de registros entre sistemas para el análisis, las alertas y la investigación de un incidente.

Protección de registros

Los usuarios, incluidos aquellos con derechos de acceso con privilegios, no deberían tener permiso para eliminar o desactivar registros de sus propias actividades. Pueden manipular potencialmente los registros de las instalaciones de procesamiento de información bajo su control directo. Por lo tanto, es necesario proteger y revisar los registros para mantener la responsabilidad de los usuarios con privilegios.

Los controles deberían tener como objetivo proteger contra cambios no autorizados en la información de registro y problemas operativos con la instalación de registro, incluidos:

a) modificaciones de los tipos de mensajes que se graban;

b) archivos de registro que se están editando o eliminando;

c) error al grabar eventos o sobreescritura de eventos grabados pasados si se excede el medio de almacenamiento que contiene un archivo de registro.

Para la protección de registros, se debería considerar el uso de las siguientes técnicas: Hash de cifrado, grabación en un archivo de solo anexión y de solo lectura, grabación en un archivo de transparencia pública.

Algunos registros de auditoría pueden ser necesarios para archivarse debido a los requisitos de retención de datos o a los requisitos para recopilar y conservar pruebas

Cuando la organización necesite enviar registros del sistema o de la aplicación a un proveedor para ayudar con la depuración o la solución de errores, los registros deberían desidentificarse siempre que sea posible mediante técnicas de enmascaramiento de datos para obtener información como nombres de usuario, direcciones de protocolo de Internet (IP), nombres de host o nombre de la organización, antes de enviarlos al proveedor.

Los registros de eventos pueden contener datos confidenciales e información de identificación personal. Deberían adoptarse medidas adecuadas de protección de la intimidad.

Análisis de registro

El análisis de los registros debería abarcar el análisis y la interpretación de los eventos de seguridad y/o privacidad de la información, para ayudar a identificar actividades inusuales o comportamientos anómalos, que pueden representar indicadores de compromiso.

El análisis de los eventos debería realizarse tomando en consideración:

a) las habilidades necesarias para los expertos que realizan el análisis;

b) determinar el procedimiento de análisis de registros;

c) los atributos necesarios por evento relacionado con la seguridad y/o privacidad;

d) Excepciones identificadas mediante el uso de reglas predeterminadas [por ejemplo, información de seguridad y gestión de eventos (SIEM) o reglas de firewall y sistemas de detección de intrusiones (IDS) o firmas de malware];

e) Patrones de comportamiento conocidos y tráfico de red estándar en comparación con la actividad y el comportamiento anómalos [análisis de comportamiento de usuarios y entidades (UEBA)];

f) resultados del análisis de tendencias o patrones (por ejemplo, como resultado del uso de análisis de datos, técnicas de big data y herramientas de análisis especializadas);

g) inteligencia de amenazas disponible.

El análisis de registros debería estar respaldado por actividades de supervisión específicas para ayudar a identificar y analizar el comportamiento anómalo, que incluye:

a) Revisar los intentos correctos e incorrectos de acceder a los recursos protegidos [por ejemplo, servidores del sistema de nombres de dominio (DNS), portales web y recursos compartidos de archivos];

b) Comprobar los registros DNS para identificar las conexiones de red salientes a servidores malintencionados, como los asociados a los

servidores de control y comandos botnet;

c) examinar los informes de uso de los proveedores de servicios (por ejemplo, facturas o informes de servicio) para determinar si hay actividad inusual en los sistemas y las redes (por ejemplo, revisando los patrones de actividad);

d) incluye registros de eventos de monitoreo físico, como entrada y salida, para Asegurar una detección y análisis de incidentes más precisos;

e) correlacionar registros para permitir un análisis eficiente y muy preciso.

Los incidentes de seguridad y/o privadad de la información sospechosos y reales deberían identificarse y estar sujetos a una investigación más exhaustiva como parte de un proceso de gestión de incidentes de seguridad y/o privacidad de la información.

6.9. ACTIVIDADES DE MONITOREO

La Universidad debe realizar actividades de monitoreo para detectar comportamientos anómalos y posibles incidentes de seguridad y/o privacidad de la información, teniendo en cuenta la normatividad vigente.

Se debería considerar la inclusión de los siguientes elementos en el sistema de supervisión:

a) tráfico de red, sistema y aplicaciones salientes y entrantes;

b) acceso a sistemas, servidores, equipos de red, sistema de supervisión, aplicaciones críticas, etc.;

c) archivos de configuración del sistema y de la red de nivel crítico o administrativo;

d) registros de herramientas de seguridad [por ejemplo, antivirus, IDS, sistema de prevención de intrusiones (IPS), filtros web, firewalls, prevención de fugas de datos];

e) registros de eventos relacionados con la actividad del sistema y de la red;

f) comprobar que el código que se está ejecutando está autorizado a ejecutarse en el sistema y que no se ha manipulado (por ejemplo, mediante recopilación para añadir código no deseado adicional);

g) uso de los recursos (por ejemplo, CPU, discos duros, memoria, ancho de banda) y su rendimiento.

La organización debería establecer una línea de base de comportamiento normal y vigilar contra esta línea de base para detectar anomalías. Al establecer una línea base, se debería tener en cuenta lo siguiente:

a) revisar la utilización de los sistemas en períodos normales y máximos;

b) hora habitual de acceso, ubicación del acceso, frecuencia de acceso para cada usuario o grupo de usuarios.

El sistema de supervisión debería configurarse con respecto a la línea base establecida para identificar el comportamiento anómalo, como:

a) terminación no planificada de procesos o aplicaciones;

b) Actividad normalmente asociada con malware o tráfico procedente de direcciones IP o dominios de red maliciosos conocidos (por ejemplo, , los asociados con los servidores de comando y control de botnet);

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 de red, niveles de latencia y fluctuación de red);

f) acceso no autorizado (real o tentativo) a sistemas o información;

g) análisis no autorizado de aplicaciones, sistemas y redes del negocioes;

h) intentos correctos e incorrectos de acceder a los recursos protegidos (por ejemplo, servidores DNS, portales web y recursos compartidos de archivos);

i) comportamiento inusual del usuario y del sistema en relación con el comportamiento esperado.

Se debería utilizar el monitoreo continuo a través de una herramienta de monitoreo. El monitoreo debería realizarse en tiempo real o en intervalos periódicos, sujeto a las necesidades y capacidades de la organización. Las herramientas de supervisión deberían incluir la capacidad de gestionar grandes cantidades de datos, adaptarse a un panorama de amenazas en constante cambio y permitir la notificación en tiempo real. Las herramientas también deberían ser capaces de reconocer firmas y datos específicos o patrones de comportamiento de red o aplicaciones.

El software de supervisión automatizada debería configurarse para generar alertas (por ejemplo, mediante consolas de administración, mensajes de correo electrónico o sistemas de mensajería instantánea) basándose en umbrales predefinidos. El sistema de alerta debería ser ajustado y entrenado en la línea de base de la organización para minimizar falsos positivos. El personal debería estar dedicado a responder a las alertas y debería estar debidamente capacitado para interpretar con precisión los posibles incidentes. Debería haber sistemas y procesos redundantes para recibir y responder a las notificaciones de alerta.

Los eventos anormales deberían comunicarse a las partes relevantes para mejorar las siguientes actividades: Auditoría, evaluación de la seguridad y/o privacidad, análisis y monitoreo de vulnerabilidades (ver 5,25). Deberían establecerse procedimientos para responder oportunamente a los indicadores positivos del sistema de vigilancia, a fin de minimizar el efecto de los eventos adversos (véase el numeral 5,26) en la seguridad y/o privacidad de la información. También deberían establecerse procedimientos para identificar y abordar falsos positivos, incluido el ajuste del software de supervisión para reducir el número de falsos positivos futuros.

Otra información

La supervisión de la seguridad y privacidad se puede mejorar mediante:

a) aprovechar los sistemas de inteligencia frente a amenazas (véase el numeral 5,7);

b) aprovechar las capacidades de aprendizaje automático e inteligencia artificial;

c) al utilizar listas de bloqueo o listas de permisos;

d) realizar una serie de evaluaciones técnicas de seguridad (por ejemplo, evaluaciones de vulnerabilidad, pruebas de penetración, simulaciones de ciberataques y ejercicios de respuesta cibernética) y utilizar los resultados de estas evaluaciones para ayudar a determinar las líneas de base o el comportamiento aceptable;

e) utilizar sistemas de supervisión del rendimiento para ayudar a establecer y detectar comportamientos anómalos; f) aprovechar los registros en combinación con los sistemas de supervisión.

Las actividades de supervisión se realizan a menudo al utilizar software especializado, como sistemas de detección de intrusiones. Se pueden configurar en una línea de base de las actividades normales, aceptables y esperadas del sistema y de la red.

El monitoreo de comunicaciones anómalas ayuda a identificar botnets (es decir, un conjunto de dispositivos bajo el control malicioso del propietario de botnet, que se suele utilizar para montar ataques distribuidos de denegación de servicio en otros equipos de otras organizaciones). Si el equipo está controlado por un dispositivo externo, existe una comunicación entre el dispositivo infectado y el controlador. Por lo tanto, la organización debería emplear tecnologías para vigilar las comunicaciones anómalas y adoptar las medidas necesarias.

6.10. SINCRONIZACIÓN DEL RELOJ

Se deberían documentar e implementar los requisitos externos e internos de representación de tiempo, sincronización fiable y precisión. Tales requisitos pueden ser legales, legales, reglamentarias, contractuales, de normas y de

supervisión interna. Se debería definir y considerar un tiempo de referencia estándar para su uso dentro de la organización para todos los sistemas, incluidos los sistemas de gestión de edificios, los sistemas de entrada y salida y otros que puedan utilizarse para ayudar en las investigaciones.

Un reloj vinculado a una emisión de hora de radio desde un reloj atómico nacional o un sistema de posicionamiento global (GPS) debería utilizarse como reloj de referencia para los sistemas de registro; una fuente de fecha y hora coherente y fiable para Asegurar la precisión de las marcas de hora. Los protocolos como el protocolo de hora de red (NTP) o el protocolo de hora de precisión (PTP) deberían utilizarse para mantener todos los sistemas conectados en red sincronizados con un reloj de referencia. ver MANUAL DE SINCRONIZACION DE RELOJ EN SERVIDOR

La organización puede utilizar dos fuentes de tiempo externas al mismo tiempo para mejorar la fiabilidad de los relojes externos y gestionar de forma adecuada cualquier variación.

La sincronización del reloj puede ser difícil cuando se utilizan varios servicios en la nube o cuando se utilizan servicios en la nube y en las instalaciones. En este caso, se debería supervisar el reloj de cada servicio y registrar la diferencia para mitigar los riesgos derivados de las discrepancias.

La configuración correcta de los relojes de computador es importante para asegurar la precisión de los registros de eventos, que puede ser requerido para investigaciones o como evidencia en casos legales y disciplinarios. Los registros de auditoría inexactos pueden obstaculizar dichas investigaciones y dañar la credibilidad de dichas pruebas.

6.11. USO DE PROGRAMAS DE UTILIDAD PRIVILEGIADOS

Se deberían tener en cuenta las siguientes directrices para el uso de programas de utilidad que pueden ser capaces de anular los controles del sistema y de la aplicación:

a) limitación del uso de programas de utilidad al número mínimo práctico de usuarios confiables y autorizados (Véase el numeral 8.2);

b) el uso de procedimientos de identificación, autenticación y autorización para programas de utilidad, incluyendo la identificación única de la persona que utiliza el programa de utilidad;

c) definir y documentar los niveles de autorización para los programas de utilidad;

d) autorización para el uso ad hoc de programas de utilidad;

e) no poner los programas de utilidad a disposición de los usuarios que tengan acceso a las aplicaciones en sistemas donde se requiera la separación de tareas;

f) eliminar o desactivar todos los programas de utilidad innecesarios;

g) como mínimo, la segregación lógica de los programas de utilidad del software de aplicación. Cuando sea práctico, separar las comunicaciones de red para dichos programas del tráfico de aplicaciones;

h) limitación de la disponibilidad de los programas de utilidad (por ejemplo, durante la duración de un cambio autorizado);

i) registro de todo uso de programas de utilidad.

6.12. INSTALACIÓN DE SOFTWARE EN SISTEMAS OPERATIVOS

Se debería tener en cuenta las siguientes directrices para gestionar de forma segura los cambios y la instalación del software en los sistemas operativos:

a) realizar actualizaciones del software operativo solo por parte de administradores formados con la autorización de administración adecuada (véase el numeral 8,5);

b) Asegurar que solo se instala código ejecutable aprobado y ningún código de desarrollo o compiladores en los sistemas operativos;

c) solo instalar y actualizar el software después de realizar pruebas exhaustivas y satisfactorias (véase el numeral 8,29 y 8,31);

d) actualizar todas las bibliotecas de origen de programas correspondientes;

e) utilizar un sistema de control de configuración para mantener el control de todo el software operativo, así como de la documentación del sistema;

f) definir una estrategia de reversión antes de implementar los cambios;

g) mantener un registro de auditoría de todas las actualizaciones del software operativo;

h) archivado de versiones antiguas de software, junto con toda la información y parámetros necesarios, procedimientos, detalles de configuración y software de soporte como medida de contingencia y durante el tiempo que el software sea necesario para leer o procesar datos archivados.

Cualquier decisión de actualizar a una nueva versión debería tener en cuenta los requisitos del negocio para el cambio y la seguridad de la versión (por ejemplo, la introducción de nuevas funciones de seguridad y privacidad de la información o el número y la gravedad de las vulnerabilidades de seguridad y/o privacidad de la información que afectan a la versión actual). Los parches de software se deberían aplicar cuando puedan ayudar a eliminar o reducir las vulnerabilidades de seguridad y/o privacidad de la información (véase el numeral 8,8 y 8,19).

El software informático puede basarse en software y paquetes suministrados externamente (por ejemplo, programas de software que utilizan módulos alojados en sitios externos), que debería monitorearse y controlarse para evitar cambios no autorizados ya que pueden introducir vulnerabilidades de seguridad y/o privacidad de la información.

El software suministrado por el proveedor y utilizado en los sistemas operativos debería mantenerse a un nivel respaldado por el proveedor. Con el tiempo, los proveedores de software dejarán de admitir versiones anteriores de software. La organización debería considerar los riesgos de confiar en software no compatible. El software de código abierto utilizado en los sistemas operativos debería mantenerse en la última versión apropiada del software. Con el tiempo, el código de código abierto puede dejar de mantenerse, pero sigue estando disponible en un repositorio de software de código abierto. La organización también debería considerar los riesgos de depender de software de código abierto no mantenido cuando se utiliza en sistemas operativos.

Cuando los proveedores participan en la instalación o actualización de software, el acceso físico o lógico solo debería darse cuando sea necesario y con la autorización adecuada. Es preciso monitorear las actividades del proveedor (véase el numeral 5,22).

La organización debería definir y aplicar reglas estrictas sobre los tipos de software que los usuarios pueden instalar.

El principio de privilegio mínimo debería aplicarse a la instalación de software en sistemas operativos. La organización debería identificar qué tipos de instalaciones de software están permitidas (por ejemplo, actualizaciones y parches de seguridad para el software existente) y qué tipos de instalaciones están prohibidas (por ejemplo, software que solo es para uso personal y software cuyo origen con respecto a ser potencialmente malintencionado es desconocido o sospechoso). Estos privilegios deberían concederse en función de las funciones de los usuarios afectados.

6.13. FILTRADO WEB

La organización debería reducir los riesgos de que su personal acceda a sitios web que contienen información ilegal o que se sabe que contienen virus o material de phishing. Una técnica para lograr esto funciona al bloquear la dirección IP o el dominio de los sitios web en cuestión. Algunos navegadores y tecnologías antimalware lo hacen automáticamente o pueden configurarse para hacerlo.

La organización debería identificar los tipos de sitios web a los que el personal debería o no tener acceso. La organización debería considerar bloquear el acceso a los siguientes tipos de sitios web:

a) sitios web que tengan una función de carga de información a menos que se permita por razones comerciales válidas;

b) sitios web maliciosos conocidos o sospechosos (por ejemplo, aquellos que distribuyen contenido de malware o phishing);

c) servidores de comando y control;

d) sitio web malicioso adquirido de inteligencia contra amenazas (véase el numeral 5,7);

e) sitios web que comparten contenido ilegal.

Antes de implementar este control, la organización debería establecer reglas para un uso seguro y apropiado de recursos en línea, incluida cualquier restricción a sitios web indeseables o inadecuados y aplicaciones basadas en web. Las normas deben mantenerse actualizadas.

Se debería impartir capacitación al personal sobre el uso seguro y adecuado de los recursos en línea, incluido el acceso a la Web.

6.14. PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN DURANTE LAS PRUEBAS DE AUDITORÍA

Deberían observarse las siguientes directrices:

a) acordar las solicitudes de auditoría para el acceso a los sistemas y datos con la dirección correspondiente;

b) acordar y controlar el alcance de las pruebas técnicas de auditoría;

c) limitar las pruebas de auditoría al acceso de solo lectura a los programas y datos. Si no se dispone de acceso de solo lectura para obtener la información necesaria, ejecutar la prueba por un administrador experimentado que tenga los derechos de acceso necesarios en nombre del auditor;

d) si se concede el acceso, establecer y verificar los requisitos de seguridad y privacidad (por ejemplo, antivirus y parches) de los dispositivos utilizados para acceder a los sistemas (por ejemplo computadores portátiles o tabletas) antes de permitir el acceso;

e) solo permitir el acceso a copias aisladas de los archivos del sistema que no sean de solo lectura y borrarlas una vez finalizada la auditoría o darles la protección adecuada si existe la obligación de conservar dichos archivos

en virtud de los requisitos de la documentación de auditoría;

f) identificar y acordar las solicitudes de procesamiento especial o adicional, como la ejecución de herramientas de auditoría;

g) la ejecución de pruebas de auditoría que puedan afectar a la disponibilidad del sistema fuera del horario laboral;

h) supervisar y registrar todos los accesos con fines de auditoría y prueba.

7. RESPONSABILIDADES Y AUTORIDADES

Los funcionarios administrativos, docentes, estudiantes, pasantes, judicantes, contratistas y/o terceros deben cumplir con la política y directrices de seguridad y privacidad de la información definidas por la Universidad Surcolombiana; así mismo, deben reportar a los propietarios de la información y otros activos asociados las violaciones a la política, directrices y/o cualquier inconsistencia o irregularidad que pueda ser generada por los usuarios.

Los líderes de procesos y propietarios de la información y otros activos de la información deben revisar periódicamente los riesgos que se identifiquen sobre el uso inadecuado de los activos.

8. DOCUMENTOS RELACIONADOS Y REGISTROS

AP-THU-DA-03 ROLES, RESPONSABILIDADES Y AUTORIDADES DE LA INSTITUCIÓN
AP-TIC-PR-11 BORRADO ACTIVOS DE INFORMACION
ES-GSPI-DA-03 GUIA FUENTES DE INFORMACIÓN DE AMENAZAS SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
ES-GSPI-DA-01 GUIA DE INTELIGENCIA DE AMENAZAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
AP-TIC-PR-06 SOPORTE TÉCNICO DE EQUIPOS INFORMÁTICOS Y PUNTOS DE RED
MANUAL DE SINCRONIZACION DE RELOJ EN SERVIDOR

CONTROL DE CAMBIO		
VERSIÓN	DOCUMENTO Y FECHA DE APROBACIÓN	DESCRIPCION DE CAMBIO
01	EV-CAL-FO-17 del 1 de septiembre del 2026	Creación documento

ELABORÓ	REVISÓ	APROBÓ
MARTHA LILIANA HERMOSA TRUJILLO Gestión Seguridad y Privacidad de la Información **Elaboró** DIEGO ANDRES CARVAJAL RUIZ Director Centro de Tecnología Información y Control Documental **Aprobó**	ALVARO TORRENTE LÓPEZ Profesional de apoyo SGC	MAYRA ALEJANDRA BERMEO Coordinador SGC