# Política de Seguridad Informática y de la Información

**UNIVERSIDAD DEL VALLE DE GUATEMALA**

Descripción breve

Documento que contiene la normativa aplicable a la Universidad del Valle de Guatemala en términos de seguridad informática

DITIC | DIRECCIÓN GENERAL DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN

|Jefatura de Seguridad

# Contenido

## 1. Antecedentes

La siguiente política está basada en las mejores prácticas utilizadas a nivel internacional, considerando como referencia la ISO 27001:2013, que facilita la guía para proteger los activos de información de las amenazas internas o externas, bien sean intencionadas, naturales o accidentales.

De igual forma, se establece que son premisas de la Universidad del Valle de Guatemala garantizar, entre otros:

a. **Confidencialidad** de la información, de manera que únicamente usuarios autorizados tengan acceso.
b. **Integridad** de la información, evitando cambios no autorizados.
c. **Disponibilidad** de la información, asegurando su acceso cuando sea requerida por usuarios debidamente autorizados y en un tiempo razonable de respuesta.
d. **Cumplimiento de las leyes** y regulaciones de acuerdo con lo establecido por la normativa de la UVG.
e. **Capacitar** a todos los colaboradores en el tema relacionado con la seguridad de la información.
f. **Cumplimiento de las obligaciones** contractuales con nuestros clientes y proveedores.

## 2. Alcance

Esta política es aplicable a estudiantes, personal académico, administrativo y de investigación, así como toda persona que por motivos contractuales tengan acceso a la información, tanto interna como externa, a través de los servicios y tecnologías que, de forma transversal, gestionan la información de Universidad del Valle de Guatemala, incluyendo sus 3 campus y al Colegio Americano del Sur, en cualquiera de los formatos existente y futuros.

## 3. Objetivo

Establecer las políticas institucionales de la Universidad del Valle de Guatemala en materia de seguridad informática y de la información que deben ser observadas y norman el acceso, disponibilidad e integridad de los sistemas de información electrónica.

### Objetivos Específicos

- Garantizar que las actividades administrativas, académica y de investigación se realizan con observancia y cumplimiento a la presente política.

- Analizar, evaluar e identificar riesgos y vulnerabilidades, así como su respectiva mitigación, tomando en consideración que los riesgos deben ser aceptados, transferidos o bien mitigados a un nivel mínimo aceptable.

- Facilitar en todas las entidades de la UVG, a través de los servicios y tecnología informática, las herramientas que respondan a las mejores prácticas de la seguridad informática y de la información.

- Informar oportunamente a los miembros de la comunidad UVG las responsabilidades que conllevan la autorización de accesos a la información en el cumplimiento de sus actividades.

## 4. Definiciones

- **Clasificación de la información**[1]: Por su tipo, la información puede ser:
    - **Confidencial:** Es la información más sensible y relevante, limitado al conocimiento de un grupo específico, normalmente implica permisos de acceso a las autoridades de la UVG. En materia de riesgo su mal intencionada o involuntaria manipulación o difusión provoca un impacto alto y se convierte en un riesgo crítico.
    - **Restringida:** Este tipo de información es de acceso a colaboradores designados por las máximas autoridades de la UVG.
    - **Interna:** Se refiere a información dirigida y disponible para Colaboradores y miembros de la comunidad de la UVG, para el desarrollo de sus actividades. La difusión y disponibilidad debe limitarse dentro de las entidades de la UVG y sin disponibilidad externa, a excepción de terceros involucrados con previa autorización de los responsables, quienes deberán haber suscrito un acuerdo de confidencialidad relacionado con no divulgarla y acompañar en todo momento a quien adquiera el acceso para su responsable custodia. En materia de riesgo, el mal uso presume un impacto medio y con riesgo medio.
    - **Pública:** Es la información disponible al público en general. En materia de riesgo, este tipo de información tiene impacto bajo y riesgo mínimo por lo que constituye la información con menor carácter crítico y sensible.
- **Activo de Información:** Son aquellos elementos que tienen valor para la UVG, que contienen datos o información y que ante su afectación podría poner en riesgo algún proceso del negocio, incluye, pero no limitado a: registros, archivos, datos, facilidades de tecnología de la información, equipos, equipos personales, instalaciones y el software licenciado por la UVG.
- **ATLASSIAN**: Suite de aplicaciones para diferentes propósitos: A) Jira Service Management, gestión de solicitudes e incidentes. En UVG esta aplicación se denomina “Service Now”. B) Jira Software: gestión de proyectos, tareas y recursos. C) Confluence, es un espacio colaborativo de documentación.
- **ATP:** Proceso de pruebas de aceptación, por sus siglas en inglés Acceptance Test Procedure
- **BCP:** Plan de continuidad del negocio (Business Continuity Plan).
- **BD:** Base de Datos Equipo Activo: cualquier dispositivo de comunicación que funcione como segregador de la señal dentro de la red.
- **Colaborador:** Persona contratada en relación de dependencia o por servicios profesionales, activo en cualquiera de las entidades de la UVG. Incluye personal administrativo, académico o de investigación.
- **Criptográficos:** técnica a través de la cual se cifra la información.
- **DAM:** monitoreo de actividades en la base de datos.
- **DGTH**: Dirección General de Gestión de Talento Humano.
- **DiTIC:** Dirección de Tecnologías de la Información y Comunicaciones.
- **DRP:** Plan de recuperación de desastres (Disaster Recovery Plan).
- **ISO/IEC 27001-2013 Anexo A** (Normativo)**:** Indica el estándar utilizado como referencia de esta política, específicamente se aplicaron las normativas del Anexo A de la misma.

[1] *Extraído de la Norma ISO 27001 - Gestión de la seguridad de la información.*

- **Malware:** programa malicioso.
- **Miembro de la Comunidad de la UVG:** Persona física que tiene relación laboral, de administración, investigación o académica con alguna o todas las entidades de la UVG.
- **OLA:** Acuerdo operativo de nivel de servicio (operational level agreement)
- **OWASP:** Proyecto abierto de seguridad de aplicaciones web.
- **PAM:** gestión de accesos privilegiados.
- **Portal Cautivo:** Pagina por medio de la cual se firma un usuario para acceder a la WiFi.
- **Ransomware**: Tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema operativo infectado y pide un rescate a cambio de eliminar esta restricción.
- **REF:** Referencia.
- **Resiliencia:** Capacidad para adaptarse a situaciones adversas.
- **Seguridad informática:** conocida como Ciberseguridad, se enfoca en la protección a la infraestructura y sistemas informáticos que, de forma transversal, directa o indirecta, se relacionan con la información digital.
- **SLA:** Acuerdo de nivel servicio, por sus siglas en inglés (service level agreement)
- **SO:** Sistema Operativo
- **Software:** Conjunto de programas que le permiten al dispositivo realizar diferentes tareas.
- **Teletrabajo:** Modalidad de trabajo a distancia.
- **UAT:** Pruebas de aceptación de usuario por sus siglas en inglés: user acceptance testing.
- **Usuario Privilegiado**: Identifica a personas a quienes se les ha conferido algún permiso especial de acceso informático.
- **Usuario:** persona que tiene acceso y utiliza las diferentes aplicaciones y sistemas aplicativos disponibles, sin privilegios.
- **UVG:** Incluye a los Campus de la Universidad del Valle de Guatemala y al Colegio Americano del Sur.
- **VPN:** red privada virtual, por medio de la cual un usuario puede acceder, desde una ubicación externa, a los sistemas de la Universidad.

## 5. POLÍTICA DE SEGURIDAD INFORMÁTICA

Se han seleccionado los siguientes objetivos de control y normativa, que adelante se desarrollan y que permiten mantener un nivel aceptable de administración de riesgos y vulnerabilidades, necesarios para garantizar que los sistemas informáticos sean seguros.

- Políticas de seguridad de la información
- Organización de la seguridad de la información
- Seguridad de los recursos humanos
- Gestión de activos
- Control de accesos
- Criptografía
- Seguridad física y el entorno
- Seguridad de las operaciones
- Seguridad de las comunicaciones
- Adquisición, desarrollo y mantenimiento del sistema
- Relaciones con los proveedores
- Gestión de incidentes de seguridad de la información
- Aspectos de seguridad de la información de la gestión de la continuidad del servicio

### Políticas de seguridad de la información

La UVG está comprometida con la protección de todos sus activos de información, consciente de que la falta de estos presume pérdidas económicas que pueden impactarle negativamente. En virtud de lo anterior, la información es uno de los activos más valiosos, por lo que se debe resguardar con la aplicación de las siguientes políticas:

P.5.1.1 La DiTIC, a través del Departamento de Seguridad Informática junto con los diferentes Líderes de la Universidad en los diferentes niveles, son responsables de concientizar a todos los usuarios, a través de capacitación continua sobre aspectos de seguridad informática y de la información, con el propósito de prepararlos sobre la responsabilidad que les corresponde en el ámbito de la seguridad informática y de la información.

P.5.1.2 La DITIC, a través del el Departamento de Seguridad Informática, es responsable de la observancia periódica de la actualización y aplicabilidad de la normativa en el entorno de la UVG para que cumplan su propósito y efecto.

P.5.1.3 La DiTIC debe facilitar a los miembros de UVG, plataformas que permitan llevar el control de los incidentes relacionados con la seguridad informática y de la información, con el propósito de ser debidamente gestionados.

P.5.1.4 Es responsabilidad de quien gestione documentos contractuales dentro de la UVG, que se contemplen, en sus cláusulas, los aspectos que permitan garantizar la seguridad informática y de la información frente a nuestros colaboradores, proveedores y terceros.

P.5.1.5 Es responsabilidad de cada dueño o responsable de cualquier activo de información su respectivo resguardo. Estos están clasificados de acuerdo con su nivel de sensibilidad expresado en la clasificación de la información.

P.5.1.6 Es responsabilidad de la DITIC establecer controles que protejan todas las infraestructuras en las que de forma transversal navega y/o se almacena toda nuestra información digital, así como de proporcionar la base de un marco pragmático de seguridad de la información, definir e implementar

con acceso restringido, un conjunto de controles mínimos de seguridad de la información, conocidos como Objetivos de Control y Normativa, establecidos dentro de este documento, siendo responsabilidad de todos los usuarios, cumplirla.

P.5.1.7 La política, los objetivos de control y la normativa se deberán comunicar a los usuarios y a las partes externas que se considere conveniente a través del Departamento de Seguridad Informática, los cuales estarán disponibles a través del sitio web de seguridad de la información, en el portal principal de cada una de las entidades que integran la UVG.

La normativa aplicable a la gestión y privacidad de la información obtenida a través de plataformas tecnológicas se encuentra contenida en *UVG.DITIC.01.003 Política de privacidad de información*[2].

***Responsabilidades específicas***

P.5.1.8 El director de la DITIC debe facilitar y junto a los Directores Ejecutivos, velar porque las unidades organizativas de tecnología de los Campus Externos implementen las medidas de seguridad de la información de la UVG, además de aprobar el sistema de controles internos y someterlo a la aprobación correspondiente. Una vez implementado, supervisar la adecuación y eficacia del entorno de control.

P.5.1.9 El Departamento de Seguridad Informática es responsable de proponer para su aprobación el marco de la política y la estrategia de seguridad informática y de su constante mantenimiento, con el propósito de garantizar la disponibilidad, integridad y confidencialidad de la información institucional. Todos los colaboradores que ejerzan funciones de liderazgo dentro de la institución deberán participar en capacitaciones específicas sobre la aplicación de esta política de manera que tengan el conocimiento necesario.

P.5.1.10 Todos los usuarios (estudiantes y colaboradores) deben completar la formación sobre seguridad de la información, proveída por DiTIC, siendo responsables de tomar decisiones informadas para proteger la información a la cual tienen acceso.

P.5.1.11 El Jefe de Seguridad Informática, también conocido como oficial de seguridad cibernética o especialista en seguridad de la información, desempeña un papel crucial en la protección de los sistemas, redes y datos en la Universidad contra amenazas cibernéticas y violaciones de seguridad. Sus funciones abarcan una amplia gama de responsabilidades para garantizar la integridad, confidencialidad y disponibilidad de la información y los activos digitales de la organización. Sus funciones principales incluyen, pero no se limitan a:

a. Gestión de políticas y procedimientos de seguridad: Desarrollar, implementar y mantener políticas, estándares y procedimientos de seguridad que guíen las prácticas seguras dentro de la organización.
b. Evaluación y gestión de riesgos: Identificar y evaluar posibles riesgos de seguridad cibernética en los sistemas y redes de la organización, desarrollando estrategias para mitigar esos riesgos.
c. Monitoreo y detección de amenazas: Utilizar herramientas y sistemas de seguridad para supervisar constantemente las actividades de la red y sistemas en busca de actividades sospechosas o maliciosas.
d. Respuesta a incidentes: Desarrollar planes de respuesta a incidentes y coordinar acciones en caso de violaciones de seguridad, ataques cibernéticos u otras amenazas.
e. Gestión de parches y actualizaciones: Coordinar con las diferentes áreas involucradas que todos los sistemas y software estén actualizados con los últimos parches de seguridad para mitigar vulnerabilidades conocidas.

[2] *Consulte este documento en su última versión en: https://bit.ly/CDI-UVG*

f. Implementación de controles de acceso: Administrar y configurar sistemas de autenticación y autorización para garantizar que solo las personas autorizadas tengan acceso a los recursos y datos críticos.
g. Educación y concientización: Capacitar a los empleados sobre prácticas de seguridad cibernética, concienciar sobre amenazas actuales y fomentar comportamientos seguros en línea.
h. Auditorías de seguridad: Realizar auditorías regulares de seguridad para evaluar la eficacia de las medidas de seguridad implementadas e identificar áreas de mejora.
i. Planes de continuidad del negocio: Verificación de la existencia e implementación para garantizar la continuidad de las operaciones en caso de interrupciones importantes causadas por ciberataques u otras situaciones.
j. Evaluación de tecnologías de seguridad: Investigar y recomendar nuevas herramientas y soluciones de seguridad que puedan fortalecer la postura de seguridad de la organización.
k. Cumplimiento normativo: Asegurarse de que la universidad cumpla con las regulaciones y estándares de seguridad relevantes.
l. Análisis forense: En el caso de incidentes de seguridad graves, realizar análisis forenses para determinar el alcance del ataque, identificar la causa raíz y tomar medidas correctivas.

En resumen, el Jefe de Seguridad Informática es responsable de salvaguardar los activos digitales de una organización y protegerla contra una amplia gama de amenazas cibernéticas, manteniendo la integridad, confidencialidad y disponibilidad de la información.

## Organización de la Seguridad de la Información

***En relación con los dispositivos propiedad de la Universidad del Valle de Guatemala***

P.5.1.12 Todos los dispositivos a los que el colaborador tenga acceso para su uso están estrictamente bajo su responsabilidad, tanto el dispositivo físico, los accesorios, como la información propiedad de la UVG, los cuales deberán ser utilizados únicamente para fines laborales para los cuales le han sido proporcionados.

P.5.1.13 El colaborador al que se le asigne un dispositivo móvil debe utilizarlo de acuerdo con lo instituido por la Dirección de Gestión de Talento Humano y demás instrucciones recibidas por su líder inmediato, siendo responsable de los riesgos de seguridad que pudieran generarle a la institución por acceso a fotografías, videos, documentos personales, aplicaciones, navegación a sitios web, entre otros.

P.5.1.14 El colaborador no debe deshabilitar o desinstalar, bajo ningún concepto, la protección contra software malicioso, antivirus u otro software autorizado e instalado por DiTIC.

P.5.1.15 Para cualquier dispositivo con acceso a redes inalámbricas, el usuario es el responsable por la conexión a redes inalámbricas que representen un riesgo de acceso no autorizado a los dispositivos bajo su responsabilidad (Redes públicas o de extraña procedencia).

P.5.1.16 La DITIC es responsable de facilitar la licencia además de la instalación del antivirus, así como su respectiva actualización.

***En relación con el uso de los dispositivos personales***

P.5.1.17 Los dispositivos personales deberán estar protegidos por una contraseña de acceso, de al menos 8 caracteres, para garantizar la seguridad de la información. Es indispensable contar con un antivirus actualizado que será responsabilidad del propietario del dispositivo.

P.5.1.18 El uso de dispositivos personales para acceder a información de la UVG se denomina “Bring Your Own Device” BYOD por sus siglas en inglés, es permitido bajo las siguientes condiciones:

a. Todos los datos de la institución que sean almacenados, transferidos o procesados en dispositivos personales son propiedad de UVG, quien mantiene el derecho a controlar esa información, aunque no sea propietaria del dispositivo, y por consiguiente puede tomar acciones para eliminar la información de dichos dispositivos, cuando así lo considere necesario. Los dispositivos deben cumplir con los controles de seguridad que establezca la UVG.

**b.** La UVG se reserva el derecho a restringir el acceso a la información de la Universidad en dispositivos personales que no cumplan con los requisitos estipulados.

**c.** La UVG administra la información con las herramientas que considere adecuadas para mejorar la experiencia del colaborador y la seguridad de los datos.

***En relación con equipos ajenos a UVG***

P.5.1.19 DITIC no tiene autorizado realizar diagnósticos o reparaciones a nivel de Software y Hardware en equipos personales que presenten problemas dentro o fuera del campus. DITIC se limitará a referirlos al centro de servicio técnico más cercano, sin asumir responsabilidad alguna sobre la decisión que tome el propietario.

***En relación con el teletrabajo[3]***

P.5.1.20 Cualquier dispositivo que la UVG facilite a sus colaboradores para realizar sus labores fuera de las instalaciones de la Universidad, es con el propósito explícito de ser utilizados estrictamente para uso laboral de acuerdo con el perfil de trabajo y descripción del puesto entregado por la DGTH.

P.5.1.21 La UVG proveerá a los colaboradores que considere necesario de la conexión segura para salvaguardar la información, en tal caso los colaboradores deberán gestionar la red privada virtual (VPN) por sus siglas en inglés, con el departamento de Operaciones de DITIC a través de la mesa de ayuda disponible.

P.5.1.22 El uso de la VPN debe ser solamente en los casos de estar fuera de los campus institucionales donde las redes no están disponibles.

P.5.1.23 Es responsabilidad del colaborador o proveedor autorizado que utilice equipo propio para trabajar con la información de la institución, contar con licencia de antivirus, sistema operativo, para hacer uso de VPN y de los recursos disponibles de la institución.

***En relación con el reporte de incidentes***

P.5.1.24 En caso de incidentes todos los colaboradores tienen a su disposición la mesa de ayuda a través de Service Now, por medio de diferentes canales, algunos de los incidentes que se pueden reportar son:

- **Robo o pérdida de equipo que pertenezca a la UVG o de tipo personal BYOD.**
- Sospecha de uso de credenciales por parte de alguna otra persona.
- Falta o incumplimiento a la política, específicamente a los objetivos de control y normativa.
- Mensajes, llamadas telefónicas o correo electrónico solicitando información personal o sus

[3] *Para más información, consulte UVG.DGTH.01.002Politica de Trabajo*

credenciales de acceso de fuentes desconocidas.
- Cualquier problema con su equipo (Hardware) o aplicaciones (Software) que de alguna forma interfiera o degrade sus servicios y le impida realizar sus labores con normalidad.

P.5.1.25 Tanto para Campus Central, Sur, Altiplano y Cas, todos los incidentes deben ser reportados de forma digital a través de:
- Plataforma Service Now
- Correo electrónico: soporte.tecnología@uvg.edu.gt
- Llamada telefónica al Departamento de Soporte Aplicativo, extensión 21551

## Seguridad de los Recursos Humanos

P.5.1.26 Es responsabilidad de la Dirección de Gestión de Talento Humano:
- Coordinar con las áreas respectivas la capacitación necesaria para la adopción de nuevas herramientas, el desarrollo de habilidades, así como competencias para el resguardo de los activos de información y la seguridad informática.
- Los acuerdos contractuales y de confidencialidad con los empleados y contratistas deberán exponer sus responsabilidades y las de la Institución para la seguridad de la información.

## Gestión De Activos

### *Inventario de activos*

P.5.1.27 Los activos asociados con la seguridad informática y de la información serán identificados y un inventario de estos será elaborado y mantenido de acuerdo con las siguientes disposiciones que incluyen, pero no limita:

- El respaldo de la información de cada dispositivo: es responsabilidad del usuario tener su copia en la nube de acuerdo con las herramientas facilitadas por DiTIC.

- Los respaldos de la información que se generan dentro de toda la infraestructura quedan bajo la responsabilidad del Departamento de Operaciones e Infraestructura.

- Toda la información digital sensible de UVG debe de ser respaldada con una programación de ejecución de backup con frecuencia diaria, semanal, quincenal mensual, trimestral, de acuerdo con las condiciones de dicha información. En el caso de respaldos específicos que requiera algún usuario, deberá ser solicitado a través de la mesa de ayuda, para su atención.

- Todos los equipos y dispositivos de la institución deberán poseer medidas de seguridad activas y actualizadas (antimalware, Antivirus, anti ransomware, entre otros) de acuerdo con las herramientas facilitadas por DiTIC.

### *Gestión de medios extraíbles*

P.5.1.28 Es responsabilidad de DITIC la implementación de controles adecuados para evitar la fuga o pérdida de información, como activo de la Institución. El departamento de Operaciones e Infraestructura deberá realizar por defecto el bloqueo de medios extraíbles como USB, CD, DVD entre otros que se utilicen con el propósito de almacenar y/o transferir información. Esta restricción

no aplica para el uso de los dispositivos externos de entrada y salida (teclado, mouse, audífonos, impresores, entre otros).

## Control De Acceso

### *De usuarios*

P.5.1.29 El usuario es responsable de la confidencialidad y uso de la cuenta asignada, sea esta individual, de servicio o colectiva. La contraseña es de uso personal e intransferible y no debe ser compartida por ningún medio, salvo excepción con aprobación de las autoridades superiores competentes o de la DGTH.

P.5.1.30 Los accesos a los sistemas de la UVG deberán ser solicitados por escrito para documentar su autorización y delegación, aplica para todas las aplicaciones.

P.5.1.31 Los derechos de acceso otorgados deben limitarse a lo que el usuario necesita para el desempeño de sus labores de acuerdo con el perfil y su hoja de descripción de trabajo asignados por la DGTH. De ser necesario se pueden dar otros accesos que no necesariamente sean parte del perfil de trabajo, previamente autorizados por la autoridad superior.

P.5.1.32 El acceso a la red y servicios que la UVG facilita, serán gestionados bajo el principio de cuentas únicas, personales e intransferibles.

P.5.1.33 El Departamento de Seguridad Informática es el encargado de atender las solicitudes de accesos a los diferentes sistemas existentes dentro de la UVG, a través de la mesa de ayuda.

P.5.1.34 La estructura de la contraseña de los usuarios debe ser: como mínimo 8 dígitos compuesto por letras, números, mayúsculas, minúsculas y caracteres especiales. La contraseña de red caduca cada 90 días como máximo.

P.5.1.35 Las contraseñas por defecto que vienen en los productos de fabricantes se deben modificar después de la instalación del activo (equipo de cómputo, servidores, SO, BD, equipo activo etc.).

P.5.1.36 La DGTH será responsable de remitir mensualmente a la DITIC un listado de colaboradores que fueron deshabilitados por inactividad para su respectivo seguimiento sea este por vacaciones, suspensión laboral por cualquier motivo que fuera con el propósito de deshabilitar la cuenta de forma temporal o definitiva de acuerdo con lo reportado por la DGTH.

P.5.1.37 Todos los usuarios que no tengan movimiento, o intervención dentro de la red por más de 15 días hábiles serán deshabilitados hasta que la DGTH envíe un memorándum o correo para su rehabilitación.

### *Usuarios privilegiados* [4]

P.5.1.38 El acceso mediante cuentas privilegiadas deberá ser reservado sólo para el personal que, por sus funciones de administración, seguridad o monitoreo de sistemas, justifique la necesidad de tener dicho tipo de acceso.

P.5.1.39 El acceso de las cuentas de usuario privilegiadas que vienen por defecto en los recursos de cómputo debe ser restringido o desactivado.

[4] *Para más información, consulte el apartado 4. Definiciones, de este documento.*

**NOTA:** Cada aplicación, módulo, plataforma o sistema cuenta con un dueño funcional y es responsable de dar autorización a los cambios que se impulsen en sus módulos, aplicaciones, sistemas, etc. así como brindar autorización a los cambios de perfiles de acceso en los módulos, sistemas, plataformas de las que es dueño funcional.

***Autenticación***

P.5.1.40 Se debe asegurar que todos los sistemas y aplicaciones requieren al menos un factor de autenticación para las aplicaciones domésticas, para los servicios en la nube deben ser de doble factor de autenticación como mínimo.

P.5.1.41 Dependiendo del valor de la información y del nivel de riesgo interno o externo a la que se encuentra expuesta la institución, la DiTIC definirá e implementará las herramientas y medios de identificación y autenticación apropiados, los cuales deberán estar habilitados en los recursos de información establecidos, a manera de restringir el acceso de acuerdo con los diferentes roles y responsabilidades del personal.

***En relación con el uso del correo electrónico***

P.5.1.42 La cuenta de correo electrónico es de uso personal e intransferible, su propósito es exclusivamente para temas laborales, siendo responsabilidad del colaborador y/o tercero salvaguardar el acceso a la información que reciba o envíe.

P.5.1.43 En todos los correos de la institución debe indicarse al pie de la página: *"La información contenida en este correo electrónico es estrictamente CONFIDENCIAL; está destinada únicamente al destinatario designado. En caso de que este mensaje haya sido recibido por error o llegue a manos equivocadas, le informamos que queda expresamente PROHIBIDO utilizar, divulgar, copiar o distribuir cualquier información contenida en él. En lugar de leerlo, se le agradecerá que lo borre inmediatamente y notifique al propietario emisor acerca del error en la entrega. Los comentarios o puntos de vista expresados en este correo electrónico son únicamente una expresión del emisor y no necesariamente representan políticas o posiciones oficiales de la entidad. Le recordamos la importancia de mantener la confidencialidad y el respeto por la PRIVACIDAD de la información conforme las leyes vigentes.".*

P.5.1.44 Cualquier usuario de cuenta de correo electrónico deberá cumplir con los siguientes lineamientos:

- Redactar los mensajes de manera clara, concisa y usando un lenguaje profesional. No se permite el uso de lenguaje inapropiado incluyendo, pero no limitado a discriminación, groserías, opiniones políticas, soez, sexuales, violencia, entre otros.
- Identificar los mensajes de acuerdo con su importancia y urgencia.
- Los archivos adjuntos de alto volumen deben enviarse de manera comprimida o hacerse disponibles a través de folders accesibles desde la red.
- En caso de duda del remitente o fuente de algún correo electrónico se debe reportar el caso a soporte aplicativo por cualquiera de los medios disponibles.
- Identificar claramente al destinatario y limitar el número de personas copiadas en el mensaje.
- Evitar el uso de destinatarios ocultos.
- Identificar de manera clara y concisa el asunto del mensaje, haciendo referencia su contenido.
- No se permite el uso de la cuenta de correo para distribución de cadenas de correo con información que no corresponda a la UVG. No se permite el envío de correos masivos, en caso de requerirlo, debe ser solicitado a las áreas correspondientes.
- Prohibido el uso del correo para fines lucrativos personales.

- El usuario puede contar con tres tipos de correo electrónico, colaborador administrativo, de investigación o académico, estudiante y pueden estar activos todos los tipos de correo a la vez. Los mismos quedan bajo la responsabilidad del usuario y su mal uso será sancionado de acuerdo con lo estipulado por la DGTH.

***En relación con el uso de las redes inalámbricas***

P.5.1.45 Es responsabilidad de la DiTIC, en coordinación con DGTH, organizar capacitaciones para el uso correcto de las redes inalámbricas existentes.

P.5.1.46 Todos los equipos capacitados para conexiones inalámbricas deberán poseer medidas de seguridad activas y actualizadas (antimalware, Antivirus, anti ransomware, entre otros).

P.5.1.47 Las redes inalámbricas disponibles pueden ser utilizadas por medio de los usuarios de red que facilitan su acceso.

P.5.1.48 Las redes inalámbricas disponibles para los invitados, visitantes y proveedores pueden ser utilizadas únicamente por terceras personas, no colaboradores, ni estudiantes, a través del portal cautivo ingresando la información solicitada para su debido registro e identificación.

P.5.1.49 Todas las personas que hagan uso de los servicios inalámbricos son responsables por su buen uso.

***En relación con el uso de internet***

UVG permite el acceso al servicio de internet, estableciendo controles que limitan su navegación abierta de forma tal que garanticen la seguridad y el uso adecuado del servicio, evitando la propagación de actividades maliciosas como malware, ransomware que, de alguna forma, directa o indirecta, ponga en riesgo el activo más importante de la UVG, así como fuga o pérdida de información.

P.5.1.50 Están restringidos los accesos a páginas relacionadas con pornografía. En el caso de acceso a música, videos, películas, streaming u otros, se autorizará de acuerdo con los perfiles y roles indicados por la DGTH.

P.5.1.51 Para todos aquellos colaboradores que por alguna razón necesitan acceso a cualquiera de estos sitios restringidos, deberán realizar su solicitud cumpliendo con los procesos de solicitud vigentes.

***Políticas y normas de uso del nodo internet***

P.5.1.52 El nodo de la Universidad del Valle de Guatemala –uvg.edu.gt–, no ejerce control alguno sobre el contenido de información que circule por él.

P.5.1.53 UVG.EDU.GT. no da garantías de tipo alguno, sea expresa o implícitamente, para el servicio que provee. Tampoco da garantías de su adecuación para uso particular. La Universidad del Valle de Guatemala no será responsable de cualquier daño que el usuario sufra. Esto incluye la pérdida de datos que resulten de atrasos, falta de entrega, entregas equivocadas, o interrupciones de servicio causada por negligencia propia o los errores u omisiones de sus usuarios.

P.5.1.54 Todos los servicios informáticos prestados por la UVG solamente pueden utilizarse para propósitos académicos, laborales, administrativos y de investigación. Cualquier mal uso, incluyendo materiales protegidos, el usuario exime a la UVG de cualquier responsabilidad o reclamo por daños

a usuarios o terceras personas resultantes. Si fuera el caso, el usuario indemnizará a la Universidad del Valle de Guatemala, por el gasto que se incurra por el manejo inadecuado de los servicios mencionados.

P.5.1.55 Cualquiera que acceda a otras redes por medio del nodo uvg.edu.gt debe acatar las reglas que rijan las mismas.

P.5.1.56 El contenido de los mensajes enviados por internet, son de completa responsabilidad del usuario emisor y en todo caso deberán basarse en la racionalidad y la responsabilidad individual. Se asume que en ningún momento dichos mensajes podrán emplearse en contra de los intereses de personas individuales, catedráticos, alumnos, personal administrativo de la Universidad, así como de ninguna otra institución, universidad o centro de investigación/académica.

## Criptografía

P.5.1.57 Todas las comunicaciones a través de las cuales viaja la información institucional, a nivel interno como externo, deben ir cifradas con las herramientas provistas por DiTIC, que garanticen las mejores prácticas para el resguardo de las comunicaciones.

## Seguridad Física y el Entorno

P.5.1.58 Para prevenir daños e interferencia por acceso físico no autorizado se deben registrar en el libro de accesos, todos aquellos ingresos al Centro de Datos, justificando el porqué, la tarea a realizar, la hora y el día de ingreso y egreso.

P.5.1.59 El acceso dentro del Centro de Datos debe ser custodiado por quien el jefe de Operaciones asigne para dicho efecto. Ninguna persona ajena al Centro de Datos puede permanecer en su interior sin permiso y acompañamiento respectivo.

P.5.1.60 No se permite la toma de video o fotografías dentro del Centro de Datos.

P.5.1.61 Las subestaciones de redes deben tener un entorno seguro y cerrado al cual solo tendrán acceso el director de la DITIC y las personas que él asigne.

P.5.1.62 Para salvaguardar la información de la institución las herramientas de Software serán aplicadas a los activos fuera o dentro de las instalaciones de acuerdo con la consideración de los diferentes riesgos en que la misma pueda estar.

P.5.1.63 Todos los dispositivos de la Universidad del Valle de Guatemala deben ser utilizados para el fin para el cual fueron asignados.

***Mantenimiento del equipo***

P.5.1.64 Es responsabilidad de DITIC el mantenimiento del equipo facilitado a los miembros de la institución, por lo que, de forma periódica, de acuerdo con su disponibilidad, los equipos serán solicitados para su mantenimiento preventivo con el propósito de que brinden un funcionamiento correcto y evitar deterioro.

P.5.1.65 Los usuarios no deben dejar sesiones abiertas mientras el equipo esté desatendido.

P.5.1.66 Todos los dispositivos de la Universidad del Valle de Guatemala se bloquearán luego de 15 minutos sin actividad.

## Seguridad de las Operaciones

***Procedimientos operativos documentados***

P.5.1.67 Los procedimientos operativos que presumen la continuidad del negocio deben ser debidamente documentados y puestos a disposición del director de área para que cualquier colaborador de la Dirección, asignado por el director, pueda utilizarlos, con el propósito de mantener la continuidad de las operaciones.

***Restricciones a la instalación de Software***

P.5.1.68 Ningún software debe ser instalado en los dispositivos propiedad de la UVG, a no ser los permitidos de acuerdo con lo estipulado por la DITIC.

P.5.1.69 Todos los colaboradores y estudiantes reciben herramientas de almacenamiento en la nube, evaluadas y aprobadas por la DITIC, por dicha razón no debe utilizar otros medios de almacenamiento de información diferentes a los que provee la institución.

***Control de Cambios***

P.5.1.70 Se debe establecer un comité de control de cambios relacionados con los sistemas informáticos, integrado por todos los jefes de la DITIC, el mismo aprueba o desaprueba los cambios de hardware y software de la institución. Dicho comité deberá tener como mínimo una reunión semanal para evaluación y priorización de cambios.

P.5.1.71 Cada actividad que represente un cambio debe implementar un proceso debidamente documentado de gestión de cambios que contenga como mínimo, pero no limitado a:

- Fecha y hora de realización
- Rollback
- Tiempo de rollback
- El plan de trabajo (Cronograma con tiempos)
- Matrices de contactos internos y externos
- Plan de comunicación
- Plan de batería de pruebas
- ATP y UAT

P.5.1.72 Todos los cambios a recursos informáticos, tales como: infraestructura de redes/comunicaciones/tecnologías de la información, sistemas de información, bases de datos, servicios de tecnología de información su respectiva documentación debe seguir los procedimientos de gestión de cambios vigentes.

P.5.1.73 No es permitido realizar dos cambios de impacto alto y de riesgo alto a la vez. A12.4 ESTÁNDARES SEGUROS DE CONFIGURACIÓN

P.5.1.74 Las distintas áreas que administran servicios informáticos internos o públicos, deben implementar configuraciones de seguridad mínima requeridas sobre la infraestructura tecnológica que administran, esto incluye seguridad en servidores, bases de datos, sistemas operativos, dispositivos de red, equipos de comunicaciones y de seguridad perimetral; en el caso de las aplicaciones propias como aplicaciones web, aplicaciones responsive y de escritorio, entre otras, se debe desarrollar en base a estándares como la guía rápida de programación segura como OWASP.

***Monitoreo de Seguridad***

P.5.1.75 El Jefe de Seguridad Informática de DiTIC, debe implementar un monitoreo constante de los recursos tecnológicos según su criticidad, apoyados con herramientas o controles para detectar con antelación, o bien en el menor tiempo posible, cualquier evento para garantizar la seguridad y la continuidad de las operaciones.

P.5.1.76 La disponibilidad de nuestros servicios debe estar garantizada con un SLA de 98.81% (Equivale a dos horas por semana como máximo de no disponibilidad de los servicios en general)

P.5.1.77 Las alertas generadas por las herramientas y/o servicios de monitoreo deben ser validados y asignados (enviadas por cualquiera de los medios disponibles SMS, E-Mail, otros) al personal correspondiente para que sean atendidos oportunamente y prevenir anomalías que puedan afectar la arquitectura tecnológica de la UVG, así como el reporte de Uptime (Disponibilidad) impactando el SLA acordado.

P.5.1.78 Se deben implementar herramientas de software que permitan auditoría para las bases de datos que registren la gestión de accesos privilegiados (PAM), además de capturar y registrar eventos en tiempo real y brindan alertas sobre violaciones de políticas, así como proporcionar evidencia forense en el caso de una violación de datos (DAM).

## Seguridad de las Comunicaciones

***Disposiciones Generales***

P.5.1.79 Con el fin de garantizar la seguridad de la información que se transmite a través de las redes de telecomunicaciones, la DiTIC debe establecer controles que incluyen, pero no se limitan a:

- Identificación, verificación, registro y aprobación de las conexiones a redes externas.
- Configuración de los dispositivos de red, a fin de garantizar que no se produzcan cambios no autorizados.
- Existencia de controles físicos de seguridad que protejan las redes y dispositivos de telecomunicaciones.
- Verificación del proceso formal del otorgamiento de acceso remoto a los sistemas de información por medio de mecanismos seguros y autorizados.

- La debida regulación y segregación del tráfico de datos entre redes.
- La habilitación de los registros de actividad de los equipos y el monitoreo de las telecomunicaciones, así como la existencia de las herramientas y procesos que permita la detección temprana y la prevención del riesgo.
- La existencia de mecanismos que limiten y controlen el acceso desde y hacia redes inalámbricas, de tal manera de permitir su uso a usuarios y dispositivos autenticados y autorizados; así como la implementación de controles criptográficos.
- La identificación de los mecanismos de seguridad, niveles de servicio y requerimientos de gestión de todos los servicios de redes. Esto también debe ser incluido dentro de los acuerdos de nivel de servicio, ya sea si son proveídos internamente o subcontratados.

P.5.1.80 Se deben hacer respaldos de las configuraciones de cada dispositivo de red de acuerdo con las factibilidades técnicas de cada uno de los equipos activos.

P.5.1.81 Se debe realizar simulacros frecuentemente, con el propósito de poner a prueba la infraestructura y su nivel de resiliencia. Asimismo, se deben implementar soluciones de software de auditorías para análisis forense de requerimientos de eventos dentro de la red.

***Seguridad del correo***

P.5.1.82 El correo electrónico debe contar con mecanismos de seguridad mínimos, como, por ejemplo: antispam, inspección y análisis sobre los adjuntos y/o enlaces antes que el usuario pueda acceder a ellos.

P.5.1.83 A cada estudiante formalmente inscrito, se le proveerá de una cuenta de correo capaz de identificar unívocamente a cada uno. Dicha cuenta, una vez el alumno egrese de la universidad solo contará con accesos restringidos.

## Adquisición, Desarrollo y Mantenimiento del Sistema

P.5.1.84 Se deben implementar controles y procedimientos, tomando en consideración, pero no limitado a lo siguiente:

- Establecimiento de una metodología para gestionar el ciclo de vida del software, apegada a las buenas prácticas internacionales de desarrollo seguro de software, en cada una de sus fases o etapas.
- Los ambientes o entornos de desarrollo y/o pruebas estarán separados del entorno de producción.
- Asegurar la privacidad y protección de los datos en los ambientes de desarrollo y/o pruebas.
- Implementar como mínimo, pero no limitado a, tres ambientes en relación con el desarrollo de aplicaciones, prueba, calidad y producción.

P.5.1.85 Para desarrollos de terceros o bien por adquisición de soluciones externas, debe tenerse en cuenta los mismos requerimientos de seguridad, bajo los estándares que indiquen las mejores prácticas de programación segura y otros estándares establecidos por la institución. Los requisitos relacionados con la seguridad de la información deben ser incluidos en los requerimientos para nuevos sistemas de información o mejoras a los sistemas de información existentes.

P.5.1.86 Las normas para el desarrollo de software y sistemas deben ser establecidas y aplicadas para desarrollos dentro de la Institución de acuerdo con el manual de normas y procedimientos del Departamento de Desarrollo.

P.5.1.87 Los cambios a los sistemas o aplicaciones deben ser controlados por el uso formal de procedimientos de control de cambios.

P.5.1.88 Los ambientes de desarrollo no deben tener información de producción para evitar la fuga o pérdida de información, los datos gestionados en escenarios de pruebas deben ser alterados y ficticios.

P.5.1.89 Para tener la aprobación sobre la publicación de cualquier software, previo deberá pasar por un riguroso proceso de pruebas, debidamente documentado, empezando por ATP (Acceptance Test Procedure) y UAT (User Acceptence Testing) finalizando con la entrega del proyecto, para ponerlo en el ambiente de producción, al área de Operaciones de la DITIC.

P.5.1.90 Es responsabilidad del área de Desarrollo en conjunto con la DGTH la coordinación de capacitaciones constantes para el adecuado uso de las aplicaciones y servicios que presta el departamento de Desarrollo.

***Gestión de actualizaciones de seguridad y vulnerabilidades***

P.5.1.91 Se debe Implementar un proceso de análisis, monitoreo y evaluación de la exposición de las vulnerabilidades de los sistemas críticos, como mínimo una vez por año, si se trata del análisis de vulnerabilidades externas. De forma interna, todas las veces que sean solicitadas por los jefes de los departamentos de Desarrollo y Seguridad Informática o el director de la DITIC, con el fin de proceder con las acciones correctivas que permitan mitigar los riesgos expuestos de dichos sistemas.

P.5.1.92 Deberán contarse con todas las actualizaciones de seguridad que apliquen, para estar adecuadamente protegido.

## Relaciones con los Proveedores

***Políticas de seguridad con terceros***

P.5.1.93 Los riesgos de ciberseguridad relacionados con terceros deben ser identificados durante el proceso de selección, validando que cuenten con buenas prácticas de ciberseguridad de acuerdo con los estándares más actualizados del mercado y lo solicitado por la UVG.

P.5.1.94 Todo tercero con acceso a los sistemas de información, red institucional, plataformas tecnológicas e información de UVG debe firmar un acuerdo de confidencialidad y contrato de servicios.

P.5.1.95 En cualquier contrato de prestación de servicios, se debe establecer los acuerdos de servicios (ANS), siendo el administrador del contrato el responsable debe monitorear su cumplimiento.

P.5.1.96 Todo tercero que, para efecto de cumplimiento del servicio, requiera acceso a los sistemas de información, red institucional, plataformas tecnológicas e información de la UVG a través de mecanismos seguros de conexión, siendo responsable de la confidencialidad y uso de la cuenta de usuario y contraseña asignada.

P.5.1.97 Los usuarios de sistemas asignados a terceros deben tener una vigencia limitada, por un periodo establecido, de acuerdo con el término del proyecto o servicio a su cargo.

P.5.1.98 Las transacciones comerciales de tipo confidencial entre UVG y terceros deben hacer uso de herramientas y mecanismos de cifrado.

P.5.1.99 Los terceros deben informar cualquier evento o incidente de ciberseguridad inmediatamente al personal de la DITIC de la UVG.

***Seguridad de servicios en la nube***

P.5.1.100 Debe cumplirse con las mejores prácticas de seguridad en la nube, considerando los diferentes aspectos establecidos en esta política incluyendo, pero no limitándose, al cifrado de la información transmitida, el almacenamiento seguro de los datos, controles de accesos, respaldos de la información y aspectos de seguridad contractuales.

## Gestión de Incidentes de Seguridad de la Información

P.5.1.101 Todo incidente de ciberseguridad debe ser tratado desde su detección hasta su resolución, mediante un procedimiento establecido para el adecuado tratamiento de incidentes.

P.5.1.102 El Jefe de Seguridad informática deberá proveer de una herramienta que apoye el proceso de atención, seguimiento y cierre de los incidentes de ciberseguridad. En la medida de lo posible, se deben emitir métricas de eficiencia en la resolución de los incidentes, permitir asignar prioridades y llevar un registro del estado de las actividades de investigación para la resolución.

P.5.1.103 Los incidentes y problemas de ciberseguridad deben ser manejados por el equipo de respuesta ante incidentes definido por UVG.

P.5.1.104 Los canales de comunicación oficiales para el reporte de incidentes son los dispuestos en la P.5.1.24 de este documento.

P.5.1.105 Todo el personal que administra la infraestructura tecnológica debe estar capacitado para la gestión de incidentes de ciberseguridad.

P.5.1.106 Se debe incluir dentro de los planes de respuesta ante incidentes de ciberseguridad, un plan de gestión de crisis en el que se incluya los procesos de evaluación de eventos, incidentes y desastres para determinar la forma en la cual UVG responderá a los sucesos, según dicho plan.

P.5.1.107 Si por alguna razón se detecta algún dispositivo conectado a la red institucional que realice actividad sospechosa maliciosa, la institución a través de la DITIC deberá tomar las medidas que crea convenientes para evitar dicha actividad.

P.5.1.108 Es responsabilidad del Departamento de Seguridad informática proponer e implementar capacitaciones que fortalezcan y mejoren los aspectos de seguridad informática además del envío periódico de cápsulas informativas que, de forma proactiva, minimicé ser víctimas de los ciberdelincuentes.

## Aspectos de Seguridad de la Información de la Gestión de la Continuidad del Servicio

Todas las unidades organizativas responsables de la provisión de servicios informáticos en la universidad, tienen la responsabilidad de:

***Creación de respaldos***

P.5.1.109 Se debe establecer un proceso de respaldo que incluya copias de la información, programas, aplicaciones, documentación, bases de datos, entre otros; incluyendo los procedimientos de recuperación. Esto debe ser aplicado como parte de las actividades previas a la realización de cambios en los sistemas o infraestructura, así como de las actividades asociadas a la continuidad de la infraestructura tecnológica que soporta los procesos críticos del negocio.

P.5.1.110 Se determinarán períodos de conservación de la información en los respaldos durante los plazos que sean definidos según las regulaciones establecidas por entes supervisores o legales y las necesidades de UVG, determinadas por el propietario de la información y el administrador del sistema.

P.5.1.111 Implementar herramientas o controles que permitan la administración de las versiones para todo el software existente, además de metodologías de integración continua.

P.5.1.112 El plan de continuidad del negocio (BCP) por sus siglas en inglés, debe contener un Plan de Contingencia y un Plan de recuperación de desastres (DRP).

***Pruebas de restauración***

P.5.1.113 Los respaldos de la información deben ser probados periódicamente mediante la implementación del proceso de recuperación de datos definido por las áreas responsables, verificando que todos los datos han sido restablecidos satisfactoriamente y de forma íntegra.

***Protección contra software malicioso***

P.5.1.114 Todos los equipos de cómputo, servidores y estaciones de trabajo deben contar con la herramienta de protección contra software malicioso.

P.5.1.115 Los usuarios deben tener acceso restringido a modificar los parámetros de configuración, solamente podrá ser ajustado/modificado por un administrador autorizado.

## 6. Cumplimiento, Revisión y Sanciones

P.6.1.1 Esta política será revisada de forma anual por DiTIC, quien propondrá las modificaciones para garantizar que las mismas sean aplicables, universales y actualizadas de acuerdo con lo regulado dentro de esta política.

P.6.1.2 El incumplimiento de esta política incluirá sanciones administrativas, relacionadas con la falta de observancia a lo dispuesto en el *GEV.CFUVG.01.001 Código de Ética, UVG.DGTH.02.001 Reglamento Interior de Trabajo y Código de Trabajo en el caso de Colaboradores, UVG.VAC.01.001 Código de Comportamiento de los estudiantes*, así como lo contemplado en las leyes aplicables del país. Para establecer el responsable de evaluar y determinar la sanción aplicable a cada caso, se considerará la intención y la gravedad del acto atendiendo la siguiente matriz.

**Matriz de Gravedad de Intención**

| | | | Intención | | |
|---|---|---|---|---|---|
| | | | **Sin dolo** | **Negligencia o dolo dudoso** | **Con Dolo** |
| | | | Conducta que evidencia que no existió voluntad para su ejecución. | Conducta que evidencia descuido o desatención a las obligaciones y en donde no existe voluntad, pero puede existir reincidencia en la ejecución. | Voluntad deliberada en la ejecución de la falta. |
| **Gravedad** | **Alta** | Conductas que dañan reputacionalmente, afectan el patrimonio de UVG o dañan a colaboradores, docentes, estudiantes o público en general. | Advertencia escrita al expediente del Colaborador / Estudiante según corresponda + sanción que establezca el responsable de evaluar el caso. | Advertencia escrita al expediente del Colaborador / Estudiante + sanción que establezca el responsable de evaluar el caso. | Advertencia escrita al expediente del Colaborador / Estudiante + sanción que establezca el responsable de evaluar el caso. |
| | **Media** | Conductas que ponen en riesgo la reputación o el patrimonio de UVG o en riesgo a colaboradores, docentes, estudiantes o público en general. | Advertencia verbal con notificación en el expediente del Colaborador / Estudiante según corresponda + sanción que establezca el responsable de evaluar el caso. | Advertencia escrita al expediente del Colaborador / Estudiante + sanción que establezca el responsable de evaluar el caso. | Advertencia escrita al expediente del Colaborador / Estudiante según corresponda + sanción que establezca el responsable de evaluar el caso. |
| | **Baja** | Incumplimiento de políticas o procedimientos básicos de su puesto. | Advertencia verbal con notificación en el expediente del Colaborador / Estudiante según corresponda + sanción que establezca el responsable de evaluar el caso. | Advertencia verbal con notificación en el expediente del Colaborador / Estudiante según corresponda + sanción que establezca el responsable de evaluar el caso. | Advertencia escrita al expediente del Colaborador / Estudiante según corresponda + sanción que establezca el responsable de evaluar el caso. |
| **Responsable de evaluar la falta y sancionar el caso:** | | | **Faltas de Estudiantes**: serán conocidas y resueltas por Secretaría General, Vicerrectoría Académica y Decanatura que corresponda<br><br>**Faltas de Colaboradores:** serán conocidas y resueltas por DGTH y Director de Departamento.<br><br>**Faltas de Contratistas:** serán conocidas y resueltas por la DGA y el Director de Departamento | | **Faltas de Estudiantes y Colaboradores y Contratistas**:<br><br>Las faltas serán elevadas al Comité de Ética para la resolución de la sanción aplicable |

## 7. Excepciones

Cualquier excepción a la presente política deberá ser analizada por la DiTIC y justificada apropiadamente en función de la necesidad de UVG.

## 8. Control de Cambios

| Versión | Fecha | Descripción del cambio |
|---|---|---|
| 1.0 | 31/07/2023 | Creación del documento. Este documento incluye la normativa relacionada con la seguridad informática e integra, actualiza y reemplaza dentro de su texto, lo contenido en los siguientes documentos: *UVG.DiTIC.01.002 Política y Normas de Uso del Nodo de Internet sin fecha de emisión y la UVG.DiTIC.01.001 Política de IT de marzo de 2010.* |