PROTOCOLO DE MANEJO Y SEGURIDAD DE LA INFORMACION
H&A-MN-TS-003

TABLA DE CONTROL

Elaborado por:	Revisado por:	Aprobado por:
_____ *Yovany Camacho Garzón* **Subgerente de IST**	_____ *Orlando Salcedo Reyes* **Vicepresidente**	_____ *Hayder Hernández Ordoñez* **Presidente**

CONTROL DE CAMBIOS

Versión No.	Fecha	Descripción de la Modificación	Autor
01	2016-05-20	Emisión Inicial – Creación del documento	Yovany Camacho Garzón

1. OBJETIVO

Determinar los lineamientos que permitan proteger la Información de H&A CONSULTING LTDA a través de acciones de aseguramiento de la Información teniendo en cuenta los requisitos legales, operativos, tecnológicos, de seguridad y de la organización alineados con el contexto de direccionamiento estratégico y de gestión del riesgo con el fin de asegurar el cumplimiento de la integridad, no repudio, disponibilidad, legalidad y confidencialidad de la información.

2. ALCANCE

La metodología descrita en este manual es aplicable para el desarrollo de estándares y prácticas organizacionales efectivas en el manejo de la gestión de la seguridad de la información en todas las áreas de trabajo que componen las verticales de la organización.

3. REFERENCIAS

- Norma Técnica Colombiana NTC ISO 9001:2008, Sistemas de Gestión de la Calidad - Requisitos.
- Norma Técnica Colombiana NTC ISO 9000:2000, Sistemas de Gestión de la Calidad – Fundamentos y Vocabulario.
- Norma Técnica Colombiana NTC ISO/IEC 27001 seguridad de la información.

4. DEFINICIONES

- **Seguridad de la información:** Hace referencia al conjunto de medidas técnicas, organizacionales y legales que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de su sistema de información.
- **Política**: Conjunto de procedimientos y medidas que se adoptan expresadas formalmente por la gerencia.
- **Lineamiento**: Descripción aclaratoria de las acciones que se llevan a cabo para lograr objetivos establecidos en las políticas.
- **Activo de información:** cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios de la organización y, en consecuencia, debe ser protegido.

- **Acuerdo de Confidencialidad:** Documento en los que los funcionarios del H&A CONSULTING o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la organización, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.
- **Análisis de riesgos de seguridad de la información:** Proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.
- **Autenticación**: es el procedimiento de comprobación de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.
- **Confidencialidad**: Es la garantía de que la información no está disponible o divulgada a personas, organizaciones o procesos no autorizados.
- **Control**: Es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye policías, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.
- **Custodio del activo de información:** Es la unidad organizacional o proceso, designado por los propietarios, encargado de mantener las medidas de protección establecidas sobre los activos de información confiados.
- **Derechos de Autor:** Es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.
- **Disponibilidad**: Es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.
- **Equipo de cómputo:** Dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos o bien compilando y correlacionando otros tipos de información.
- **Incidente de Seguridad:** Es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencia, el número de veces ocurrido o el origen (interno o externo).
- **Integridad**: Es la protección de la exactitud y estado completo de los activos.
- **Inventario de activos de información:** Es una lista ordenada y documentada de los activos de información pertenecientes la compañía.
- **Licencia de software:** Es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.

- **Medio removible:** Es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información dentro de los que se incluyen cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras.
- **Perfiles de usuario:** Son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.
- **Propiedad intelectual:** Es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.
- **Propietario de la información:** Es la unidad organizacional o proceso donde se crean los activos de información.
- **Recursos tecnológicos:** Son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de H&A CONSULTING LTDA.
- **Registros de Auditoría:** Son archivos donde son registrados los eventos que se han identificado en los sistemas de información, recursos tecnológicos y redes de datos de la organización. Dichos eventos pueden ser, entre otros, identificación de usuarios, eventos y acciones ejecutadas, terminales o ubicaciones, intentos de acceso exitosos y fallidos, cambios a la configuración, uso de utilidades y fallas de los sistemas.
- **Responsable por el activo de información:** Es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.
- **Sistema de información:** Es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por el H&A CONSULTING LTDA o de origen externo ya sea adquirido por la organización como un producto estándar de mercado o desarrollado para las necesidades de ésta.

- **Software malicioso:** Es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.
- **Terceros:** Todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la organización.
- **Vulnerabilidades:** Son las debilidades, hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por la organización (amenazas), las cuales se constituyen en fuentes de riesgo.

5. POLITICA

La dirección de H&A CONSULTING LTDA, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información (SGSI) buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la organización. Para H&A CONSULTING LTDA, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Organización según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinados por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la organización.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de H&A CONSULTING LTDA.
- Garantizar la continuidad del negocio frente a incidentes.

- H&A CONSULTING LTDA ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

A continuación se establecen 11 objetivos de seguridad que soportan el SGSI de H&A CONSULTING LTDA:

OBJETIVOS

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.
- H&A CONSULTING LTDA protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.
- H&A CONSULTING LTDA protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- H&A CONSULTING LTDA protegerá su información de las amenazas originadas por parte del personal.
- H&A CONSULTING LTDA protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- H&A CONSULTING LTDA controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- H&A CONSULTING LTDA implementará control de acceso a la información, sistemas y recursos de red.
- H&A CONSULTING LTDA garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- H&A CONSULTING LTDA garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- H&A CONSULTING LTDA garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- H&A CONSULTING LTDA garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Organización, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

6. TRATAMIENTO DE DATOS PERSONALES

Para garantizar la adecuada protección de los datos personales que administra H&A CONSULTING LTDA, en cumplimiento con lo dispuesto en el artículo 15 de la Constitución Política de Colombia que consagra el derecho de cualquier persona de conocer, actualizar y rectificar los datos personales que existan sobre ellos en bancos de datos o archivos de la entidad, así como lo señalado en Ley 1266 de 2008, Ley 1581 de 2012 y el Decreto Reglamentario 1377 de 2013, que regulan el derecho de Habeas Data; la entidad está comprometida con el cumplimiento de los derechos de sus clientes, empleados y cualquier otra persona natural, estableciendo para ello los siguiente:

- Legalidad: El tratamiento dado a los datos personales es actividad reglada sujeta a la Ley.
- Finalidad: La administración de datos personales debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley. La finalidad debe informársele al titular de la información previa o concomitantemente con el otorgamiento de la autorización, cuando ella sea necesaria o en general siempre que el titular solicite información al respecto.
- Veracidad o calidad de los registros o datos: La información contenida en las bases de datos de la entidad debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.
- Libertad: Para el tratamiento de datos que no ostenten la calidad de públicos en términos de la ley, se debe contar con un consentimiento previo, expreso e informado de su titular o persona autorizada.
- Acceso y circulación restringida: Los datos personales, salvo la información pública, no podrán ser accesibles por Internet o por otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o los usuarios autorizados conforme a la ley. Se debe garantizar el derecho del titular de la información a obtener en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.
- Seguridad: La información contenida en las bases de datos de la entidad deberá contar con las medidas de seguridad técnicas que sean necesarias para garantizar la seguridad de los registros evitando su adulteración, pérdida, consulta o uso no autorizado.
- Confidencialidad: H&A CONSULTING LTDA debe garantizar la reserva de la información de los datos que no ostentan la calidad de públicos en términos de la ley, aun después de finalizada su relación con el titular de la información.

- Uso de los datos: los Datos suministrados por los clientes para los diferentes procesos realizados bajo manejo de base de datos serán usados exclusivamente para dicho fin, no se utilizaran para hacer promociones Comerciales o algo distinto a su fin.

DERECHOS DE LOS TITULARES DE DATOS PERSONALES

Los titulares de la información tienen derecho, entre otros a:

- Acceder de forma permanentemente a la información de los datos personales que estén bajo el control de H&A CONSULTING LTDA. Mediante mecanismos sencillos y ágiles.
- Para las consultas cuya periodicidad sea mayor a una por cada mes calendario, H&A CONSULTING LTDA podrá cobrar al titular los gastos de envío, reproducción y, en su caso, certificación de documentos.
- Conocer, actualizar y rectificar sus datos personales frente a los responsables del tratamiento o encargados del tratamiento.
- Solicitar prueba de la autorización otorgada al responsable del tratamiento salvo cuando expresamente la ley lo exceptúe como requisito para el tratamiento.
- Ser informado por el responsable del tratamiento o el encargado del tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales.
- Presentar ante la superintendencia de industria y comercio quejas por infracciones a lo dispuesto en la presente ley y las demás normas que la modifiquen, adicionen o complementen.
- Revocar la autorización y/o solicitar la supresión del dato cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la superintendencia de industria y comercio haya determinado que en el tratamiento el responsable o encargado han incurrido en conductas contrarias a esta ley y a la constitución.

Los derechos anteriormente enunciados podrán ejercerse por las siguientes personas, de manera oral y/o escrita siempre se acredite la autenticidad de la petición:

- Por el titular, quien deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición el responsable.
- Por sus causahabientes, quienes deberán acreditar tal calidad.
- Por el representante y/o apoderado del titular, previa acreditación de la representación o apoderamiento.
- Por estipulación a favor de otro o para otro.

ADMINISTRACIÓN DE LAS BASES DE DATOS

Las bases que contengan datos personales deben cumplir con las condiciones de seguridad requeridas para evitar su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. La responsabilidad de garantizar dichas condiciones de seguridad será del dueño de la base de datos respectiva. Para tal efecto, entiéndase por dueño de la base de datos, el proceso que en H&A CONSULTING LTDA se encuentra autorizado para efectuar modificaciones de la base de datos respectiva.

INSCRIPCIÓN DE BASES DE DATOS

H&A CONSULTING LTDA deberá inscribir las bases que contengan datos personales en el Registro Nacional de Base de Datos de la Superintendencia de Industria y Comercio.

7. RESPONSABILIDADES FRENTE A LA SEGURIDAD DE LA INFORMACIÓN Y AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

RESPONSABILIDADES DE LA GERENCIA DE TECNOLOGÍA DE SISTEMAS DE INFORMACIÓN

- Establecer, mantener y divulgar las políticas y procedimientos de servicios de tecnología, incluida esta política de seguridad de información y todos sus capítulos, el uso de los servicios tecnológicos en toda la organización de acuerdo a las mejores prácticas y lineamientos de la alta gerencia de la organización y directrices.
- Mantener la custodia de la información que reposa en los diferentes sistemas de información, bases de datos y aplicativos de la organización.
- Informar de los eventos que estén en contra de la seguridad de la información y de la infraestructura tecnológica de la organización a la alta gerencia y las diferentes gerencias de H&A CONSULTING LTDA, así como a los entes de control e investigación que tienen injerencia sobre la organización.
- Proporcionar medidas de seguridad físicas, lógicas y procedimentales para la protección de la información digital de la organización.
- Aplicar y hacer cumplir la Política de Seguridad de la Información y sus componentes.
- Administrar las reglas y atributos de acceso a los equipos de cómputo, sistemas de información, aplicativos y demás fuentes de información al servicio de H&A CONSULTING LTDA.
- Analizar, aplicar y mantener los controles de seguridad implementados para asegurar los datos e información gestionados en la organización.

- Resolver de común acuerdo con las áreas y los propietarios de la información los conflictos que se presenten por la propiedad de la información al interior de la organización. Esto incluye los posibles medios de acceso a la información, los datos derivados del procesamiento de la información a través de cualquier aplicación o sistema, los datos de entrada a las aplicaciones y los datos que son parte integral del apoyo de la solicitud.
- Habilitar/Deshabilitar el reconocimiento y operación de Dispositivos de Almacenamiento externo de acuerdo con las directrices emitidas de parte de la Alta gerencia y las diferentes gerencias.
- Implementar los mecanismos de controles necesarios y pertinentes para verificar el cumplimiento de la presente política.
- Garantizar la disponibilidad de los servicios y así mismo programar o informar a todos los usuarios cualquier problema o mantenimiento que pueda afectar la normal prestación de los mismos; así como gestionar su acceso de acuerdo a las solicitudes recibidas de las diferentes gerencias.
- Establecer, mantener y divulgar las políticas y procedimientos de los servicios de tecnología, incluidos todos los capítulos que hacen parte de esta Política, en toda la organización de acuerdo a las mejores prácticas y directrices de la Entidad.
- Determinar las estrategias para el mejoramiento continuo del servicio tecnológico, la optimización de los recursos tecnológicos, las mejoras en los sistemas de información.
- Brindar el soporte necesario a los usuarios a través de los canales de mesa de ayuda actualmente implementados en la organización.

RESPONSABILIDADES DE LOS PROPIETARIOS DE LA INFORMACIÓN

Son propietarios de la información cada uno de los funcionarios así como los gerentes de área donde se genera, procesa y mantiene información, en cualquier medio, propia del desarrollo de sus actividades.

- Valorar y clasificar la información que está bajo su administración y/o generación.
- Autorizar, restringir y delimitar a los demás usuarios de la organización el acceso a la información de acuerdo a los roles y responsabilidades de los diferentes funcionarios, contratistas o practicantes que por sus actividades requieran acceder a consultar, crear o modificar parte o la totalidad de la información.
- Determinar los tiempos de retención de la información en conjunto con él grupo de Gestión Documental y Correspondencia y las áreas que se encarguen de su protección y almacenamiento de acuerdo a las determinaciones y políticas de la entidad como de los entes externos y las normas o leyes vigentes.

- Determinar y evaluar de forma permanente los riesgos asociados a la información así como los controles implementados para el acceso y gestión de la administración comunicando cualquier anomalía o mejora tanto a los usuarios como a los custodios de la misma.
- Acoger e informar los requisitos de esta política a todos los funcionarios, contratistas y practicantes en las diferentes dependencias de la organización.

RESPONSABILIDADES DE LOS FUNCIONARIOS, CONTRATISTAS Y PRACTICANTES USUARIOS DE LA INFORMACIÓN

- Utilizar solamente la información necesaria para llevar a cabo las funciones que le fueron asignadas, de acuerdo con los permisos establecidos o aprobados en el Contrato.
- Manejar la Información de la organización y rendir cuentas por el uso y protección de tal información, mientras que este bajo su custodia. Esta puede ser física o electrónica e igualmente almacenada en cualquier medio.
- Proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido
- Evitar la divulgación no autorizada o el uso indebido de la información.
- Cumplir con todos los controles establecidos por los propietarios de la información y los custodios de la misma.
- Informar a sus superiores sobre la violación de estas políticas o si conocen de alguna falta a alguna de ellas.
- Proteger los datos almacenados en los equipos de cómputo y sistemas de información a su disposición de la destrucción o alteración intencional o no justificada y de la divulgación no autorizada.
- Reportar los Incidentes de seguridad, eventos sospechosos y el mal uso de los recursos que identifique.
- Proteger los equipos de cómputo, de comunicaciones y demás dispositivos tecnológicos designados para el desarrollo de sus funciones. No está permitida la conexión de equipos de cómputo y de comunicaciones ajenos a la organización a la red Institucional, ni el uso de dispositivos de acceso externo a Internet o de difusión de señales de red que no hayan sido previamente autorizadas por la gerencia de tecnología de sistemas de información.
- Usar software autorizado que haya sido adquirido legalmente por la organización. No está permitido la instalación ni uso de software diferente al Institucional sin el consentimiento de sus superiores y visto bueno de la gerencia de tecnología de sistemas de información.
- Divulgar, aplicar y el cumplir con la presente Política.
- Aceptar y reconocer que en cualquier momento y sin previo aviso, la Alta gerencia de la organización puede solicitar una inspección de la información a su cargo sin importar su

ubicación o medio de almacenamiento. Esto incluye todos los datos y archivos de los correos electrónicos institucionales, sitios web institucionales y redes sociales propiedad de la organización, al igual que las unidades de red institucionales, computadoras, servidores u otros medios de almacenamiento propios de la organización. Esta revisión puede ser requerida para asegurar el cumplimiento de las políticas internamente definidas, por actividades de auditoría y control interno o en el caso de requerimientos de entes fiscalizadores y de vigilancia externos, legales o gubernamentales.

- Proteger y resguardar la información personal que no esté relacionada con sus funciones en la organización. H&A CONSULTING LTDA no es responsable por la pérdida de información, desfalco o daño que pueda tener un usuario al brindar información personal como identificación de usuarios, claves, números de cuentas o números de tarjetas débito/crédito.

8. LINEAMIENTOS POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Lineamiento 1: Uso de contraseñas y usuarios
Expone las condiciones, normas y procedimientos necesarios para fijar los requisitos que se deben cumplir por cualquier funcionario, contratista o practicante de la organización para obtener acceso a los sistemas de información, hardware y software propiedad del H&A CONSULTING LTDA.

Lineamiento 2: Uso del servicio de correo electrónico
Concientiza a los funcionarios, contratistas o practicantes de la organización de los riesgos asociados con el uso de correo electrónico y presenta las normas y protocolos a seguir para el buen uso de este servicio.

Lineamiento 3: Uso del servicio de internet / intranet
Concientiza a los funcionarios, contratistas o practicantes de la organización de las buenas prácticas a seguir sobre las normas de uso del servicio de Internet/Intranet, así como el conocimiento de los riesgos asociados por el uso indebido de los mismos.

Lineamiento 4: Uso de servicio de mensajería instantánea
Concientiza a los funcionarios, contratistas o practicantes de la organización de las buenas prácticas a seguir sobre las normas y el uso del servicio de mensajería instantánea, así como el conocimiento de los riesgos asociados por el uso indebido de los mismos.

Lineamiento 5: Uso de dispositivos de almacenamiento externo
Describe el uso permitido de los dispositivos de almacenamiento externo en H&A CONSULTING LTDA y las restricciones en su empleo al interior de la organización.

Lineamiento 6: Uso de dispositivos de captura de imágenes y/o grabación de video
Define el acceso y el uso de cámaras fotográficas, cámaras de video y demás dispositivos que permitan el registro de imágenes, fotografías y/o video en H&A CONSULTING LTDA.

Lineamiento 7: Uso de escritorios y pantallas despejadas
Define los mecanismos necesarios que se deben aplicar en la organización con el fin de proteger la información física residente en los escritorios y puestos de trabajo y la información digital almacenada en los computadores e infraestructura técnica a disposición de todos los funcionarios, contratistas o practicantes para el normal desarrollo de las actividades.

Lineamiento 8: Uso de dispositivos móviles
Define los mecanismos necesarios que se deben aplicar en la organización con el fin de proteger la información física residente en Los dispositivos móviles asignados a los funcionarios de H&A CONSULTING LTDA para el normal desarrollo de las actividades.

Lineamiento 9: Copias de respaldo de la información
Define los mecanismos necesarios que se deben aplicar en la organización con el fin de la generación de copias de respaldo y almacenamiento de su información crítica, proporcionando los recursos necesarios y estableciendo los procedimientos y mecanismos para la realización de estas actividades.

Lineamiento 10: gestión de vulnerabilidades
Define los mecanismos necesarios que se deben debe implementar para el análisis de vulnerabilidades de la infraestructura tecnológica, a través de un plan de pruebas que permita identificar y tratar los riesgos que puedan comprometer la seguridad de la información o que puedan afectar la prestación de los servicios de H&A CONSULTING LTDA.

LINEAMIENTO 1: USO DE USUARIOS Y CONTRASEÑAS

La asignación de usuarios y contraseñas es un permiso que H&A CONSULTING LTDA otorga a sus funcionarios, contratistas o practicantes con el fin de que tengan acceso a los recursos tecnológicos como a las plataformas y sistemas de información que permiten la operación, consulta y resguardo de la información institucional.

Los objetivos específicos de los lineamientos para el uso de usuarios y contraseñas son:

- Presentar a todos los funcionarios y contratistas de H&A CONSULTING LTDA responsables de la asignación, creación y modificación de usuarios y contraseñas las directrices a seguir y verificar que se cumplan a cabalidad con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información del H&A CONSULTING LTDA.
- Concientizar a todos los funcionarios, contratistas o practicantes sobre los riesgos asociados con el uso de las credenciales de acceso (usuario y contraseña) y las consecuencias de exponer de manera inadecuada la identidad ante cualquier tercero, en el entendido que los usuarios y claves asignados a cada funcionario, contratista o practicante son personales e intransferibles.
- Asegurar el correcto manejo de la información privada de la organización.

La asignación de credenciales: usuarios como contraseñas (Clave o Password) a los diferentes funcionarios, contratistas o practicantes así como su desactivación de los sistemas se harán de acuerdo a los procedimientos establecidos y según sea solicitado por la alta gerencia, las gerencias de área o por los grupos de Talento Humano y Gestión Contractual.

Las cuentas de usuario son para uso personal e intransferible y por ende son de entera responsabilidad del funcionario, contratista o practicante al que se le asigne.

Las cuentas de usuario (usuario y clave) son sensibles a mayúsculas y minúsculas, es decir que estas deben ser tecleadas como se definan.

De ser necesaria la divulgación de la cuenta de usuario y su contraseña asociada, debe solicitarlo por escrito y dirigido a la gerencia de tecnología de sistemas de información.

Si se detecta o sospecha que las actividades de una cuenta de usuario puede comprometer la integridad y seguridad de la información, el acceso a dicha cuenta será suspendido temporalmente y será reactivada sólo después de haber tomado las medidas necesarias a consideración de la gerencia de tecnología de sistemas de información.

TIPOS DE CUENTAS DE USUARIO

Todas las cuentas de acceso a las plataformas tecnológicas como a los sistemas de información y aplicaciones son propiedad de la organización. Para efectos del presente lineamiento, se definen dos tipos de cuentas:

a) Cuenta de Usuario de Sistema de Información: Son todas aquellas cuentas que sean utilizadas por los usuarios para acceder a los diferentes sistemas de información. Estas cuentas permiten

el acceso para consulta, modificación, actualización o eliminación de información, y se encuentran reguladas por los roles de usuario de cada Sistema de Información en particular.

b) Cuenta de Administración de Sistema de Información: Corresponde a la cuenta de usuario que permite al administrador del Sistema, plataforma tecnológica o base de datos realizar tareas específicas de usuario a nivel administrativo, como por ejemplo: agregar/modificar/eliminar cuentas de usuario del sistema. Usualmente estas cuentas están asignadas para su gestión por parte de la gerencia de tecnología de sistemas de información.

El gerente del área de tecnología de sistemas de información deberá contar con la lista de las contraseñas sensibles para la administración de los sistemas de información, plataformas tecnológicas y bases de datos.

Estas cuentas de usuario igualmente deben mantener las siguientes políticas:

1. Todas las contraseñas de administradores deben ser cambiadas al menos cada 6 meses.
2. Todas las contraseñas de usuario de sistema de información deben ser cambiadas al menos cada 6 meses.
3. Todas las contraseñas deben ser tratadas con carácter confidencial.
4. Las contraseñas de ninguna manera podrán ser transmitidas mediante servicios de mensajería electrónica instantánea ni vía telefónica.
5. Se evitará mencionar y en la medida de lo posible, teclear las contraseñas en frente de otros.
6. Se evitará el revelar contraseñas en cuestionarios, reportes o formularios.
7. Se evitará el utilizar la misma contraseña para acceso a los sistemas operativos y/o a las bases de datos u otras aplicaciones.
8. Se evitará el activar o hacer uso de la utilidad de recordar clave o recordar Password de las aplicaciones.

Uso apropiado de usuarios y contraseñas:

- Usar las credenciales de acceso sobre los sistemas otorgados exclusivamente para fines laborales y cuando sea necesario en cumplimiento de las funciones asignadas.
- Cambiar periódicamente las contraseñas de los sistemas de información o servicio tecnológicos autorizados.

Uso indebido del servicio de usuarios y contraseñas:

- Permitir el conocimiento de las claves a terceros.
- Almacenar las credenciales de acceso en libretas, agendas, post-it, hojas sueltas, etc. Si se requiere el respaldo de las contraseñas en medio impreso, el documento generado deberá ser único y bajo resguardo.
- Almacenar las credenciales sin protección, en sistemas electrónicos personales (Tablets, memorias USB, teléfonos celulares, agendas electrónicas, etc.).
- Intentar acceder de forma no autorizada con otro usuario y clave diferente a la personal en cualquier sistema de información o plataforma tecnológica.
- Usar identificadores de terceras personas para acceder a información no autorizada o suplantar al usuario respectivo.
- Utilizar su usuario y contraseña para propósitos comerciales ajenos a la organización.
- Intentar modificar o modificar los sistemas y parámetros de la seguridad de los sistemas de la red de H&A CONSULTING LTDA.

Responsabilidades de los funcionarios, contratistas y practicantes con usuarios y contraseñas asignados

- Conocer, adoptar y acatar este lineamiento.
- Velar por la seguridad de la información a la que tenga acceso a través de las credenciales asignadas y a los sistemas de información autorizados para su acceso.
- Cerrar totalmente su sesión de trabajo para evitar el uso de su identidad, cuando se retire del equipo en que se encuentre laborando.
- Dar aviso a la gerencia de tecnología de sistemas de información, a través de los medios establecidos, de cualquier fallo de seguridad, incluyendo su uso no autorizado, pérdida de la contraseña, suplantación, etc.

Monitoreo:

- Los administradores de los sistemas de información, bases de datos y plataformas tecnológicas pueden efectuar una revisión periódica de los accesos exitosos y no exitosos y al número de intentos efectuados a dichos sistemas para determinar posibles accesos indebidos o no autorizados.

- El área de tecnología de sistemas de información podrá revisar las bitácoras y registros de control de los usuarios que puedan afectar la operación de cualquier sistema o plataforma.

LINEAMIENTO 2: USO DEL SERVICIO DE CORREO ELECTRÓNICO DEL H&A CONSULTING LTDA

El correo electrónico es un servicio basado en el intercambio de información a través de la red y el cual es provisto por el H&A CONSULTING LTDA para los funcionarios, contratistas, practicantes previamente autorizados para su acceso.

Los objetivos específicos de los lineamientos para el uso del correo electrónico son:

- Incentivar el uso del servicio de correo electrónico para fines estrictamente laborales del H&A CONSULTING LTDA.
- Asegurar el correcto manejo de la información privada de la organización por parte de los funcionarios, contratistas o practicantes de la organización.
- Garantizar la confidencialidad, la privacidad y el uso adecuado y moderado de la información a través de este servicio.

El acceso al servicio de correo electrónico es un privilegio otorgado por H&A CONSULTING LTDA a sus funcionarios, contratistas y practicantes y el mismo sobrelleva responsabilidades y compromisos para su uso.

H&A CONSULTING LTDA a criterio propio puede otorgar el acceso a los servicios de correo electrónico para la realización de actividades institucionales al personal de planta, contratistas y proveedores. El acceso incluye la preparación, transmisión, recepción y almacenamiento de mensajes de correo electrónico y sus adjuntos. La Alta gerencia y las diferentes gerencias o Coordinadores tienen la autonomía de otorgar y solicitar el acceso de sus funcionarios, contratistas o practicantes a este servicio.

Se encuentra disponible un acceso externo sobre la página web. Este sistema está pensado exclusivamente para aquellos funcionarios, contratistas o practicantes que por cualquier motivo, en un determinado momento, no puedan hacer uso del cliente de correo electrónico.

Las credenciales de los usuarios serán desactivadas de los sistemas de acuerdo a los procedimientos establecidos y según sea solicitado por La Alta gerencia y las diferentes gerencias o por los grupos de Talento Humano y Gestión Contractual.

TIPOS DE CUENTAS DE CORREO ELECTRÓNICO

Todas las cuentas de correo electrónico que existen en el servicio de correo de H&A CONSULTING LTDA son propiedad de la organización.

CREACIÓN EMAIL CORPORATIVO

Para la creación de los correos corporativos se debe tener en cuenta los siguientes aspectos:

- Se escribe las claves de acceso las cuales solo el área de sistemas y tecnología de la información genera con mínimo 12 dígitos entre numérico y alfanumérico las cuales deben de ser almacenadas y guardadas en un lugar seguro (plantilla Excel con clave de ingreso para cada caso). Está información es manejada únicamente por la alta Gerencia (Presidencia, Vicepresidencia) y el Personal encargado del proceso de tecnología y Sistemas.
- Ingresando a la dirección del sistema solicita la clave de acceso al cpanel.
- Después de ingresar los datos, se deberá seleccionar la opción Cuentas de Email.

Siguiendo las políticas de calidad de H&A CONSULTING LTDA para la creación de correos electrónicos se ha establecido la siguiente estructura:

- Alta Dirección y Gerencias: Comenzar con la letra inicial del primer nombre en minúscula seguido por el primer apellido completo en minúscula como se muestra a continuación:

  Hernando **Pérez=** hperez@haconsultingeu.com

  En caso contrario que se encuentre otra persona con este correo se tomarán las dos primeras letras iniciales del primer nombre en minúscula seguido por el primer apellido completo en minúscula como se muestra a continuación:

  Hernando **Pérez=** heperez@haconsultingeu.com

  Nota: para la creación de los correos electrónicos de los consultores de la empresa también se deben crear de la forma como se ha mencionado anteriormente. Lo anterior debido a la naturaleza del cargo que así lo requiere.

- Para los demás empleados de la compañía: Iniciar con el nombre del área como se muestra a continuación:

Sistemas= sistemas@haconsultingeu.com

- El espacio asignado para cada email y la contraseña de cada correo es asignado por la coordinación de Tecnología y Sistemas de Información de la empresa o la Alta Gerencia de la compañía, dependiendo de la naturaleza del cargo.

Uso apropiado de los servicios de correo electrónico de H&A CONSULTING LTDA

- Conservar normas de respeto, confidencialidad y criterio ético por parte de todos los funcionarios, contratistas y practicantes con acceso a este servicio.
- Usar el correo electrónico Institucional exclusivamente para fines laborales: para la difusión o el envío de circulares, memorandos, oficios y archivos de trabajo, cuando sea necesario en cumplimiento de las funciones asignadas.
- Redactar los contenidos de un mensaje de correo electrónico de tal manera que sea serio, claro, conciso, cortés y respetuoso.
- Ingresar a las cuentas de correo de cada usuario a través de los medios que la organización destina, que en este caso son los clientes de correo electrónico instalados en cada máquina. Cada funcionario, contratista o practicante tendrá asignada una credencial de acceso conformada por un usuario y una clave asignada por el Grupo de Soporte Tecnológico a través de los procedimientos establecidos.

Uso indebido del servicio de correo electrónico del H&A CONSULTING LTDA

- Participar en la difusión de “cartas en cadenas”, en esquemas piramidales o de propagandas dentro y fuera de la organización.
- Realizar intentos no autorizados para acceder a otra cuenta de correo electrónico Institucional.
- Revelar o publicar cualquier información clasificada o reservada del H&A CONSULTING LTDA.
- Descargar, enviar, imprimir o copiar documentos o contenidos en contra de las leyes de derechos de autor.
- Copiar ilegalmente o reenviar mensajes que hayan sido restringidos por parte del usuario o el emisor.
- Descargar cualquier software o archivo sin tomar las medidas de precaución para evitar el acceso de virus en las redes y equipos informáticos.
- Utilizar expresiones difamatorias o groseras en contra de individuos, clientes o entidades públicas o privadas. Los mensajes enviados a través de este servicio no pueden contener

material insidioso, ofensivo, obsceno, vulgar, racista, pornográfico, subversivo u otro material no formal.

- Enviar información clasificada o reservada de H&A CONSULTING LTDA por medio de canales no seguros (no codificados) como es Internet y/o las cuentas de correo de uso público (gmail, hotmail, yahoo, etc.). El correo electrónico está sujeto a las mismas leyes, políticas y prácticas que se aplican a la utilización de otros medios de comunicación, tales como servicios telefónicos y medios impresos.
- Participar en actividades que puedan causar congestión o interrupción en los servicios de comunicación de H&A CONSULTING LTDA o la normal operación de los servicios de correo electrónico.
- Enviar correos SPAM de cualquier índole.
- Reenviar correos con contenido PHISING.
- Usar seudónimos y enviar mensajes anónimos, así como aquellos que consignen títulos, cargos o funciones no oficiales
- Utilizar el correo electrónico para propósitos comerciales ajenos a la organización.
- Intentar modificar o modificar los sistemas y parámetros de la seguridad de los sistemas de la red de H&A CONSULTING LTDA
- Utilizar mecanismos y sistemas que intenten ocultar o suplantar la identidad del emisor de correo.
- Usar correos públicos para la recepción, envió o distribución de información pública clasificada o reservada propia de H&A CONSULTING LTDA.
- Configurar y conectar los clientes de correo electrónico con los sitios de redes sociales o con fuentes RSS que no sean autorizadas por H&A CONSULTING LTDA.
- Distribuir listas de direcciones de correo personales sin expresa autorización de sus dueños.

El uso inapropiado o el abuso en el servicio de correo electrónico ocasionan la desactivación temporal o permanente de las cuentas. La desactivación de la cuenta lleva consigo la imposibilidad de acceder a los mensajes de correo que estén en ese momento en el servidor y la imposibilidad de recibir nuevos mientras no vuelva a ser activada.

Responsabilidades de los funcionarios, contratistas y practicantes que sean usuarios de los servicios de correo electrónico de H&A CONSULTING LTDA

- Cuidar y revisar el contenido de los correos electrónicos que se envíen a través de su cuenta. El uso no autorizado de una cuenta de correo electrónico es ilegal y constituye una violación de la Política de la organización.

- Usar correctamente las credenciales de ingreso (usuario y clave) asignadas. La cuenta de correo que proporciona la organización es personal e intransferible, por lo que no debe compartirse con otras personas.
- Cerrar totalmente la sesión de lectura y envío de correos para evitar el uso de su identidad, cuando se retire del equipo en que se encuentre configurada la cuenta de correo.
- Dar aviso al Grupo de tecnología de sistemas de información, a través de los medios establecidos, de cualquier fallo de seguridad en su cuenta de correo, incluyendo su uso no autorizado, pérdida de la contraseña, suplantación, etc.
- Responsabilizarse por la información o contenido que sea transmitido a través de la cuenta de correo asignada; Los usuarios del servicio deben considerar que los mensajes enviados a un destinatario pueden ser re-enviados a cualquier número de cuentas de correo de otros individuos o grupos.
- Descargar, verificar y resguardar la información recibida a través de este servicio en su buzón local de correo electrónico, de ser este configurado, en el cliente de correo instalado en su equipo de cómputo.

Monitoreo

- H&A CONSULTING LTDA tiene el derecho a acceder y revelar los contenidos electrónicos de los correos electrónicos institucionales de sus funcionarios, contratistas y practicantes y estos deben dar su consentimiento a H&A CONSULTING LTDA en caso de que algún ente fiscalizador a nivel interno o externo requiera esta información. Priman las exigencias de carácter legal o disciplinario.
- El Administrador del Servicio o el Grupo de tecnología de sistemas de información pueden monitorear en línea el acceso y uso de los servicios Institucionales, o revisar el contenido de los equipos e información Institucional almacenados en cualquier momento, con las autorizaciones pertinentes para asegurar la integridad y confidencialidad de la información; Igualmente se efectúa una revisión periódica del tráfico de mensajes sobre los canales de comunicación como prevención de ingreso de mensajes tipo SPAM o PHISING, ingreso de virus sobre las redes y equipos informáticos, verificación de volúmenes de archivos anexos que puedan afectar la operación del sistema.
- El área de tecnología de sistemas de información puede monitorear el cumplimiento de las directrices institucionales en el momento que así lo considere o le sea requerido, con las autorizaciones pertinentes para asegurar la integridad y confidencialidad del sistema.

LINEAMIENTO 3: USO DEL SERVICIO DE INTERNET/INTRANET DEL H&A CONSULTING LTDA

Los objetivos específicos del uso de servicio de internet/intranet son:

- Incentivar el uso del servicio de Internet/Intranet para fines estrictamente laborales de H&A CONSULTING LTDA.
- Asegurar el correcto manejo de la información privada de la organización.
- Garantizar la confidencialidad, la privacidad y de uso adecuado y moderado dela información a través de este servicio.

El servicio de Internet/Intranet es un servicio de gran importancia en el mundo laboral, de conocimiento y negocios basado en el acceso a diferentes fuentes de información en distintas ubicaciones a través de sistemas de cómputo interconectados en red a nivel local y mundial.

El acceso al servicio de Internet/Intranet es un permiso otorgado por H&A CONSULTING LTDA a sus funcionarios, contratistas o practicantes y así mismo sobrelleva responsabilidades y compromisos para su uso. Se espera que los usuarios de este servicio conserven normas de buen uso, confidencialidad y criterio ético.

La alta gerencia y las diferentes gerencias tienen la autonomía de otorgar y solicitar el acceso de sus funcionarios, contratistas o practicantes a este servicio, de acuerdo al procedimiento vigente

El ingreso a este servicio se realiza por medio de la plataforma que la organización destina, que para este caso es el navegador de internet instalado en cada máquina.

El punto de inicio para acceder a este servicio se hace desde la página web institucional a través de la dirección: https://www.haconsultingeu.com/

USO APROPIADO DEL SERVICIO DE INTERNET/INTRANET

Todos los funcionarios, contratistas y practicantes con autorización al uso y acceso a estos servicios deben:

- Utilizar este servicio exclusivamente para fines laborales.
- Conservar normas de respeto, confidencialidad y criterio ético por parte de todos los funcionarios, contratistas o practicantes con acceso a este servicio.
- Descargar documentos o archivo tomando las medidas de precaución para evitar el acceso de virus en las redes y equipos informáticos.

USO INDEBIDO DEL SERVICIO DE INTERNET/INTRANET:

- Acceder a sitios de juegos o apuestas en línea.
- Acceder a sitios de divulgación, descarga o distribución de películas, videos, música, real audio, webcams, emisoras online, etc.
- Acceder y/o descargar material pornográfico u ofensivo.
- Utilizar software o servicios de mensajería instantánea (chat) y redes sociales no instalados o autorizados por el área de tecnología de sistemas de información.
- Compartir en sitios web información propia de H&A CONSULTING LTDA clasificada como reservada o clasificada sus usuarios, funcionarios, contratistas o practicantes.
- Emplear este servicio para la recepción, envió o distribución de información pública clasificada o reservada de H&A CONSULTING LTDA a través de servicios y cuentas de correo públicos.
- Realizar intentos no autorizados para acceder a otra cuenta de usuario de este servicio.
- Cargar, descargar, enviar, imprimir o copiar archivos, software o contenidos en contra de las leyes de derecho de autor.
- Utilizar el servicio de Internet/Intranet para propósitos comerciales ajenos a H&A CONSULTING LTDA.
- Intentar o modificar las opciones de configuración y/o parámetros de seguridad de los navegadores instalados por H&A CONSULTING LTDA.
- Interferir intencionalmente con la operación normal de cualquier website o portal en Internet.
- Comprar o vender artículos personales a través de sitios web o de subastas en línea.
- Acceder a sitios de contenido multimedia (videos, música, emisoras online, etc.) debido al alto consumo de canal de comunicaciones. Únicamente se autorizara el acceso a aquellos funcionarios, contratistas o practicantes que por sus actividades requieran monitorear estos sitios externos y tengan previa aprobación del Jefe Inmediato y la autorización ante el área de tecnología de sistemas de información.
- Publicar o enviar opiniones personales, declaraciones políticas y asuntos no propios de la organización, dirigidos a funcionarios, contratistas o practicantes y público en general, del sector oficial, de otras compañías y organizaciones, a través de este servicio.
- Descargar, instalar y configurar navegadores distintos a los permitidos por el área de tecnología de sistemas de información.

Responsabilidades de los Usuarios de Internet/Intranet en H&A CONSULTING LTDA:

- Conocer, adoptar y acatar esta política cada vez que haga uso de este servicio.

- Usar correctamente sus credenciales de ingreso (usuario y clave). La cuenta de acceso que proporciona la organización es personal e intransferible, por lo que no debe proporcionarse a otras personas.
- Dar aviso al área de tecnología de sistemas de información a través de los medios establecidos de cualquier fallo de seguridad de su cuenta, incluyendo su uso no autorizado, pérdida de la contraseña, bloqueo, etc.
- Proteger los derechos de autor de la información obtenida a través de este servicio. Se recomienda citar la fuente (página web) en los documentos o informes generados con información obtenida por este medio.

Monitoreo:

- Los funcionarios, contratistas y practicantes deben estar al tanto que se registra por cada usuario las visitas a los diferentes sitios y se registra estos eventos en archivos de auditoria tanto en los computadoras, propias o contratadas, como en los servidores donde se administran estos servicios.
- El área de tecnología de sistemas de información planifica periódicamente una revisión de los archivos de auditoría, las configuraciones y registros de cada una de las máquinas y navegación en Internet-Intranet.
- Si se determina que alguna de las páginas previamente restringidas por el área de tecnología de sistemas de información es requerida para el desempeño de funciones de algún funcionario, contratista o practicante esta será habilitada únicamente con el consentimiento y solicitud de su jefe directo y con el visto bueno del área de tecnología de sistemas de información.
- Los usuarios del servicio deben considerar que algunos sitios web no son seguros, especialmente los que hacen suplantación de entidades a los bancos y/o emisores de tarjetas de crédito (PHISING) por lo que se recomienda confirmar esta información directamente con las mismas entidades. Igualmente no se debe proveer información personal ni laboral a sitios de dudosa validez. H&A CONSULTING LTDA no es responsable por la pérdida de información, desfalco o daño que pueda tener un usuario al acceder a sitios de suplantación o al brindar información personal como identificación de usuarios, claves, números de cuentas o números de tarjetas débito/crédito al hacer el uso de este servicio.

LINEAMIENTO 4: USO DEL SERVICIO MENSAJERÍA INSTANTÁNEA

El acceso al servicio de mensajería instantánea es un permiso otorgada por H&A CONSULTING LTDA a sus funcionarios, contratistas o practicantes y la misma sobrelleva responsabilidades y

compromisos para su uso. Se espera que los usuarios conserven normas de buen uso, confidencialidad y criterio ético.

Los objetivos específicos del uso de servicio de mensajería instantánea son:

- Incentivar el uso del servicio de mensajería instantánea para fines estrictamente laborales del
- H&A CONSULTING LTDA.
- Asegurar el correcto manejo de la información privada de los usuarios y de la organización
- Garantizar la confidencialidad, la privacidad y el uso adecuado y moderado del mismo.

Este servicio es suministrado para los funcionarios, contratistas y practicantes, previamente autorizados para su uso, con el propósito de agilizar el trato entre los mismos a lo largo y ancho de la entidad, independiente de su ubicación física o geográfica.

Este servicio es una potente herramienta para realizar conferencias virtuales además de permitir compartir el escritorio del computador como las aplicaciones residentes en el mismo. Su uso es recomendado para presentaciones en tiempo real, entrenamientos remotos, web conferencias y reuniones en línea.

El ingreso a este servicio se realiza por medio de la plataforma que la organización destina para este caso por medio del software instalado en cada máquina y/o a través del navegador de internet residente en cada computador.

Como todo servicio, que basa su operación en el manejo de información, H&A CONSULTING LTDA promueve el uso prudente y mesurado de este servicio para apoyar las operaciones y comunicaciones propias de la organización.

Uso apropiado del servicio de Mensajería Instantánea:

- Usar el servicio de mensajería instantánea institucional exclusivamente para fines laborales.
- Transferir archivos que no tengan información sensible o reservada de H&A CONSULTING LTDA. Se debe revisar previamente que cualquier archivo a enviar esté libre de virus.
- Abstenerse de compartir información o datos personales a través de este servicio. No es aconsejable incluir información personal como contraseñas o números de tarjetas de crédito, cuentas bancarias e incluso un número de teléfono en cierta manera confidencial.
- Compartir por medio de este canal mensajes concisos, breves y veraces.
- Mantener su estado actualizado en el sistema de modo que los demás usuarios sepan si están o no disponibles y si pueden o no contactarle.

Uso indebido del servicio de mensajería instantánea:

- Emplear el servicio de mensajería instantánea Institucional para extensas conversaciones personales.
- Expresar opiniones difamatorias, ofensivas, obscenas, vulgar, racistas, calumniadoras y sexuales sobre superiores, compañeros o subalternos. Lo mismo aplica para usuarios, proveedores y demás entidades con quien haya comunicación. Esto puede comprometer la reputación y su credibilidad tanto de índole personal como institucional.
- Emplear las comunicaciones instantáneas con fines políticos, religiosos o comerciales.
- Realizar cualquier tipo de acoso, difamación, calumnia, con intención de intimidar, insultar o cualquier otra forma de actividad hostil.
- Compartir por medio de este canal información clasificada o reservada de H&A CONSULTING LTDA, de sus funcionarios, contratistas o practicantes
- Realizar intentos no autorizados para acceder a otra cuenta de usuario de este servicio.
- Compartir documentos o archivos que sean ajenos a la operación de la organización.
- Intentar o modificar las opciones de configuración y/o parámetros de seguridad de los clientes de mensajería instantánea instalados por H&A CONSULTING LTDA.
- Descargar, instalar y emplear sistemas de mensajería instantánea distintos al definido por H&A CONSULTING LTDA y administrado por el área de tecnología de sistemas de información. Los sistemas no autorizados incluyen pero no se limitan a: Yahoo! Messenger, AOL Instant Messenger (AIM), MSN Messenger, Whatsapp, eBuddy, ICQ, MySpace y Google Talk.

El uso inapropiado o el abuso en el servicio de mensajería instantánea ocasionaran la desactivación temporal o permanente de las cuentas.

Responsabilidades de los funcionarios, contratistas y practicantes usuarios del servicio de mensajería instantánea:

- Conocer, adoptar y acatar este lineamiento cada vez que haga uso de este servicio.
- Usar correctamente sus credenciales de ingreso (usuario y clave). La cuenta de acceso que proporciona la organización es personal e intransferible, por lo que no debe proporcionarse a otras personas.
- Dar aviso al área de tecnología de sistemas de información a través de los medios establecidos de cualquier fallo de seguridad de su cuenta, incluyendo su uso no autorizado, olvido de la contraseña, bloqueo, etc.
- Todos los mensajes compartidos y documentos archivos compartidos o descargados quedan bajo responsabilidad del dueño de la cuenta.

- Cada jefe de área es responsable de revisar y autorizar o desautorizar cada requerimiento de acceso de sus funcionarios, contratistas o practicantes a este servicio. Solicitudes aprobadas de acceso deben ser sometidas de acuerdo con el procedimiento vigente para este caso.
- Los usuarios del servicio deben considerar que los mensajes instantáneos pueden ser guardados por su interlocutor. Una de las partes que participa en la conversación puede copiar y pegar la conversación entera en un documento de texto. Este servicio de mensajería instantánea permiten incluso archivar mensajes completos

Monitoreo:

- Los funcionarios, contratistas o practicantes deben estar al tanto de que se registra por cada usuario los mensajes y llamadas enviadas y recibidas en archivos de auditoria tanto en los computadoras, propias o contratadas, como en los servidores donde se administran estos servicios.
- El área de tecnología de sistemas de información planifica periódicamente una revisión de los archivos de auditoría, las configuraciones y registros de cada una de las máquinas.

LINEAMIENTO 5: USO DE DISPOSITIVOS DE ALMACENAMIENTO EXTERNO

El uso de medios de almacenamiento externo a los disponibles en los diferentes equipos de cómputo, unidades de red compartidas y servidores de la entidad, constituyen una herramienta que sirve para la transferencia rápida y directa de información entre los funcionarios, contratistas o practicantes de la organización que a la vez puede exponer información confidencial y sensible de la entidad a diversos riesgos y peligros.

Los objetivos específicos del uso de dispositivos de almacenamiento externo son:

- Concientizar a los funcionarios, contratistas o practicantes de la organización sobre los riesgos asociados con el uso de los medios de almacenamiento, tanto para los sistemas de información como para la infraestructura tecnológica de la organización.
- Asegurar el correcto manejo de la información digital que reposa en la organización.
- Delimitar el uso de estos medios de almacenamiento en las diferentes áreas de H&A CONSULTING LTDA.

H&A CONSULTING LTDA es consciente que este tipo de herramientas son muy útiles para el resguardo y transporte de información pero igualmente son elementos que permiten extraer información sin dejar huella física ni registro de dicha acción; Por esta razón H&A CONSULTING LTDA define los compromisos frente al uso de Dispositivos de Almacenamiento Externo para asegurarse de que la información propietaria, adquirida o puesta en custodia en la entidad no está supeditada a fuga, uso no autorizado, modificación, divulgación o pérdida y que esta debe ser protegida adecuadamente según su valor, confidencialidad e importancia.

El uso de dispositivos de almacenamiento externo está permitido en H&A CONSULTING LTDA para los funcionarios, contratistas y practicantes; en general los funcionarios, contratistas o practicantes de la organización, con el fin de facilitar el compartir y transportar información que no sea de carácter clasificado ni reservado de la organización dentro de las normas y responsabilidades del manejo de información institucional.

Los dispositivos de almacenamiento de uso externo comprenden las unidades que se pueden conectar como una memoria USB, por medio de un cable de datos, mediante una conexión inalámbrica directa a cualquier equipo de cómputo de H&A CONSULTING LTDA. Entre estos, se pueden encontrar pero no se limitan a:

- Memorias Flash USB
- Reproductores portátiles MP3/MP4
- Cámaras con conexión USB
- iPhones/Smartphones
- SD Cards/ Mini SD Cards/ Micro SD Cards.
- PDAS / Tablets
- Dispositivos con tecnología Bluetooth.
- Tarjetas Compact Flash
- Discos duros de uso externo

Nota: El acceso y empleo de servicios de almacenamiento de archivos On Line, es decir, aquellas unidades virtuales de almacenamiento personal por medio de internet, en las cuales se incluye pero no se limitan los servicios de Skydrive, Dropbox, Rapidshare, GigaSize, MediaFire, 4shared, etc.; están prohibidos.

Uso indebido de dispositivos de almacenamiento externo:

- Almacenar o transportar información clasificada o reservada de H&A CONSULTING LTDA.

- Ejecutar cualquier tipo de programa no autorizado por la organización desde cualquiera de las unidades de almacenamiento en mención.
- Descargar cualquier archivo sin tomar las medidas de precaución para evitar el acceso de virus en las redes y equipos informáticos.
- Utilizar mecanismos y sistemas que intenten ocultar o suplantar la identidad del usuario de alguno de estos medios de almacenamiento.
- Emplear dispositivos de almacenamiento externo con el fin de almacenar o exponer información sensible o reservada de los usuarios o funcionarios, contratistas o practicantes de la organización.

El área de tecnología de sistemas de información puede en todo momento y en cualquier área o dependencia de la organización operar, almacenar, adquirir o retirar dispositivos de almacenamiento externo que les permita garantizar la seguridad de la información de H&A CONSULTING LTDA.

Responsabilidades de los usuarios de dispositivos de almacenamiento externo:

- Usar de manera responsable la información a su cargo y de los dispositivos de almacenamiento externo que emplee para el transporte de dicha información.
- Velar porque los medios de almacenamiento externo estén libres de software malicioso, espía o virus para lo cual deberá realizar una verificación de dichos dispositivos cada vez que sea conectado a un equipo de cómputo de la organización por medio del software de protección dispuesto para tal fin.

Monitoreo:

- Todos los eventos realizados sobre los dispositivos de almacenamiento externo, conectados a cualquier equipo de cómputo de la organización, podrán ser auditados con el ánimo de registrar y controlar las actividades realizadas sobre cada uno de estos, la ubicación y el usuario que los empleó. Los intentos de habilitar el uso de estos dispositivos donde su uso ha sido denegado o no autorizado igualmente podrán ser registrados.
- Las entradas de software malintencionado, de espionaje o virus podrán ser detectadas inmediatamente e informadas al administrador de la red de la organización.
- Se pueden generar informes periódicos sobre el uso de todos los elementos en H&A CONSULTING LTDA para permitir la evaluación del "uso racional de los dispositivos" y que estos sean permitidos, a fin de incrementar los niveles de seguridad para proteger la información de la organización.

LINEAMIENTO 6: USO DE DISPOSITIVOS DE CAPTURA DE IMÁGENES Y/O GRABACIÓN DE VIDEO

Los objetivos específicos del uso de dispositivos de captura de imágenes y/o grabación de video son:

- Concientizar a los funcionarios, contratistas, practicantes y demás personas vinculadas con la organización sobre los riesgos asociados al uso de dispositivos de registros de imagen y/o video, en las instalaciones de la organización.
- Fortalecer las medidas de seguridad en las áreas de H&A CONSULTING LTDA, que gestionan documentos e información de la organización.
- Dar cumplimiento a las directrices determinadas en la Política de Seguridad de la Información de la organización.
- Restringir el uso de este tipo de dispositivos en áreas de manejo de información y documentación clasificada o reservada.

Entre los dispositivos de captura de imágenes y/o grabación de video se pueden encontrar pero no se limitan a:

- Cámaras Fotográficas
- Videocámaras
- Celulares.
- iPhones/Smarthphones
- PDAS/Tablets.
- WebCams
- Scanners
- Impresoras
- Multifuncionales

Nota: La captura de imágenes y/o grabación de video por parte de los ciudadanos o visitantes de la Entidad está prohibida.

No se permite la captura de imágenes y/o grabación de video en las instalaciones o sedes de H&A CONSULTING LTDA, así como del personal por parte de la ciudadanía, funcionarios, contratistas y practicantes de la organización, sin previa autorización de la alta gerencia.

El acceso y uso de equipos fotográficos y de video para fines Institucionales, prensa o de comunicación a H&A CONSULTING LTDA debe ser autorizado previamente.

Con el único propósito de brindar protección en las áreas de H&A CONSULTING LTDA, del personal, documentos, información y activos en estas áreas alojados, los únicos dispositivos de registro audiovisual permitidos son las cámaras de seguridad que la organización designe.

En el caso de equipos de cómputo de H&A CONSULTING LTDA que cuenten con webcams integradas y los dispositivos de videoconferencia su uso es exclusivo para videoconferencias institucionales al interior de las dependencias y áreas antes señaladas.

Responsabilidades de los funcionarios, contratistas y practicantes usuarios de dispositivos de captura de imágenes y/o grabación de video:

- Adoptar, poner en práctica, socializar, y acatar estos lineamientos.
- Usar los dispositivos de captura de imágenes y/o grabación de videos que sean de su propiedad o le hayan sido asignadas para el desempeño de sus actividades de acuerdo a lo estipulado anteriormente.
- Abstenerse de fotografiar, escanear, grabar o copiar digitalmente información sensible, clasificada o reservada de la organización.
- Cumplir con todos los controles establecidos por los propietarios de la información y los custodios de la misma.
- Informar a sus superiores sobre la violación de estos lineamientos o si conocen de alguna falta a alguna de ellas.

Monitoreo:

- H&A CONSULTING LTDA puede controlar el acceso de dispositivos de captura de imágenes y/o grabación de video a sus instalaciones en las entradas a cada una de sus sedes a nivel nacional, por medio del personal de vigilancia y seguridad dispuesto en cada uno de los puntos de ingreso de la entidad.
- El monitoreo permanente de uso y manipulación de dispositivos de captura de imágenes y/o grabación de video, es efectuado a través de los sistemas de video vigilancia instalados en las diferentes áreas y sedes de la organización.
- H&A CONSULTING LTDA requerirá y mantendrá bajo custodia del personal de vigilancia y seguridad los dispositivos de captura de imágenes y/o grabación de video en las dependencias restringidas y determinadas en esta Política a cualquier persona que ingrese a las mismas y durante el tiempo que permanezca al interior de las mismas.

LINEAMIENTO 7: USO DE ESCRITORIOS Y PANTALLAS DESPEJADAS

La política de escritorios y pantallas despejadas es extensiva para todos los funcionarios, contratistas y practicantes de H&A CONSULTING LTDA y apoya en la seguridad de la información sensible o crítica de la organización.

Los objetivos específicos de este capítulo relacionado con el uso de escritorios y pantallas despejadas son:

- Garantizar la confidencialidad, la privacidad y el uso adecuado y moderado de la información.
- Crear conciencia sobre los riegos asociados al manejo de información tanto física como digital y la manera de reducirlos aplicando los lineamientos aquí determinados.
- Especificar las recomendaciones y pautas necesarias para mantener las pantallas y escritorios organizados y controlando el reposo de información clasificada o reservada a la vista.
- Dictar las pautas para mantener organizado y resguardado los documentos digitales y correos electrónicos en los computadores puestos a disposición de todos los usuarios de los sistemas de información y estructura tecnológica de H&A CONSULTING LTDA.

Este lineamiento se define en el uso adecuado y ordenado de las áreas de trabajo desde el punto de vista físico como tecnológico entendiéndose para tal fin como escritorio el espacio físico o puesto de trabajo asignado a cada funcionario, contratista o practicante de la organización y pantalla, el área de trabajo virtual sobre el sistema operativo de su computador, que contiene tanto sus carpetas electrónicas como los archivos y accesos a los diferentes aplicativos Institucionales.

El uso y conservación de los puestos de trabajo (escritorios) y de los fondos de escritorio de sus computadores (pantallas) es una responsabilidad de cada uno de los funcionarios, contratistas y practicantes que tengan acceso a la información de H&A CONSULTING LTDA, sea de manera temporal o indefinida, en el normal desarrollo de sus actividades. Para su definición y aplicación se define de la siguiente manera:
Escritorios:

- Se deben dejar organizados los puestos y áreas de trabajo, entendiéndose por esto el resguardo de documentos con información clasificada o reservada evitando que queden a la vista o al alcance de la mano de personal ajeno a la misma.
- En la medida de lo posible los documentos con información clasificada o reservada debe quedar bajo llave o custodia en horas no laborables.
- Se debe evitar el retiro de documentos clasificados o reservados de la organización y en el caso de ser necesario se debe propender por su protección fuera de la organización y su pronta devolución al mismo.

- Se deben controlar la recepción, flujo envío de documentos físicos en la organización por medio de registro de sus destinatarios desde el punto de correspondencia.
- Se debe restringir el fotocopiado de documentos fuera del horario normal de trabajo y fuera de las instalaciones de la organización. De ser necesario se debe autorizar el retiro de dichos documentos y garantizar su protección y confidencialidad fuera.
- Al imprimir o fotocopiar documentos con información clasificada o reservada, esta debe ser retirada inmediatamente de las impresoras o multifuncionales utilizadas para tal fin. Y no debe ser dejada desatendida sobre los escritorios.
- No se debe enviar ni recibir documentos clasificados o reservados por medio de Fax.
- No se debe reutilizar papel que contenga información clasificada o reservada.

Pantallas:

- Los computadores o estaciones de trabajo deben ser bloqueados por los usuarios al retirarse de los mismos y los mismos deben ser desbloqueados por medio del usuario y contraseña asignado para su acceso a los mismos. Es responsabilidad del usuario, asegurar que el equipo tenga la protección adecuada.
- Las áreas de trabajo virtuales “pantallas” del computador deben tener el mínimo de iconos visibles, limitándose estos a los accesos necesarios para la ejecución de la ofimática, accesos a sistemas de información, a carpetas y unidades de red necesarios para la ejecución de las actividades.
- Los documentos digitales deben ser organizados en carpetas y evitar dejarlos a la vista en las pantallas de los computadores.
- Los funcionarios, contratistas y practicantes al retirarse de la organización deben apagar los computadores asignados. Queda fuera de esta indicación los servidores y estaciones de trabajo utilizados para acceso remoto. Las sesiones activas se deben terminar cuando el usuario finalice las actividades programadas.
- El fondo de pantalla de cada computador es único para todas las estaciones de trabajo y para todos los usuarios y puede ser cambiado únicamente por el área de tecnología de sistemas de información o por solicitud de la alta gerencia. Para el resto de las áreas, estos cambios deben ser solicitados y validados por la alta gerencia.

Monitoreo:

El área de tecnología de sistemas de información sin previo aviso puede realizar brigadas de monitoreo para verificar el estado de los computadores, monitores y escritorios virtuales y generar el respectivo informe de lo encontrado.

LINEAMIENTO 8: USO DE DISPOSITIVOS MÓVILES

La política de uso de dispositivos móviles aplica a todos los funcionarios, contratistas y practicantes de H&A CONSULTING LTDA y apoya en la seguridad de la información sensible o crítica de la organización.

Los objetivos específicos de este capítulo relacionado con el uso de dispositivos móviles son:

- Garantizar la confidencialidad, la privacidad y el uso adecuado y moderado de la información.
- Crear conciencia sobre los riegos asociados al manejo de información a través de los dispositivos móviles y la manera de reducirlos aplicando los lineamientos aquí determinados.
- Especificar las recomendaciones y pautas necesarias para mantener tanto los dispositivos como la información protegida.
- Dictar las pautas para mantener la operación, y transmisión de la información registrada en los dispositivos móviles.

Responsabilidades del área de tecnología de sistemas de información:

- Determinar y avalar las opciones de protección de los dispositivos móviles institucionales que hagan uso de los servicios provistos por H&A CONSULTING LTDA.
- Establecer las configuraciones aceptables para los dispositivos móviles institucionales que hagan uso de los servicios provistos por H&A CONSULTING LTDA.
- Determinar los métodos de protección de acceso (por ejemplo, contraseñas o patrones) para los dispositivos móviles institucionales que serán entregados a los usuarios. Se debe configurar estos dispositivos para que pasado un tiempo de inactividad pasen automáticamente a modo de suspensión y, en consecuencia, se active el bloqueo de la pantalla el cual requerirá el método de desbloqueo configurado.
- Activar la opción de cifrado de la memoria de almacenamiento de los dispositivos móviles institucionales haciendo imposible la copia o extracción de datos si no se conoce el método de desbloqueo.
- Configurar la opción de borrado remoto de información en los dispositivos móviles institucionales, con el fin de eliminar los datos de dichos dispositivos y restaurarlos a los valores de fábrica, de forma remota, evitando así divulgación no autorizada de información en caso de pérdida o hurto.

- Implementar una solución de copias de seguridad para la información contenida en los dispositivos móviles institucionales; dichas copias deben acogerse a la Política de Copias de Respaldo.
- Instalar un software de antivirus en los dispositivos móviles institucionales que hagan uso de los servicios provistos por el H&A CONSULTING LTDA.
- Activar los códigos de seguridad de la tarjeta SIM para los dispositivos móviles institucionales antes de asignarlos a los usuarios y almacenar estos códigos en un lugar seguro.

RESPONSABILIDADES DE LOS USUARIOS:

- Los usuarios deben evitar usar los dispositivos móviles institucionales en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.
- No deben modificar las configuraciones de seguridad de los dispositivos móviles institucionales bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega.
- Evitar la instalación de programas desde fuentes desconocidas; se deben instalar aplicaciones únicamente desde los repositorios oficiales de los dispositivos móviles institucionales.
- Aceptar y aplicar la nueva versión de las actualizaciones que sean notificadas en los dispositivos móviles asignados para su uso.
- Evitar hacer uso de redes inalámbricas de uso público, así como deben desactivar las redes inalámbricas como WI-FI, Bluetooth, o infrarrojos en los dispositivos móviles institucionales asignados.
- Evitar conectar los dispositivos móviles institucionales asignados por puerto USB a cualquier computador público, de hoteles o cafés internet, entre otros.
- Abstenerse de almacenar videos, fotografías o información personal en los dispositivos móviles institucionales asignados

Monitoreo:

El área de tecnología de sistemas de información sin previo aviso puede realizar brigadas de monitoreo para verificar el estado de los dispositivos móviles y generar el respectivo informe de lo encontrado.

LINEAMIENTO 9: COPIAS DE RESPALDO DE LA INFORMACIÓN

Las áreas propietarias de la información, con el apoyo del área de tecnología de sistemas de información, encargada de la generación de copias de respaldo, definirán la estrategia a seguir y los periodos de retención para el respaldo y almacenamiento de la información. Así mismo, H&A CONSULTING LTDA velará porque los medios magnéticos que contienen la información crítica sean almacenados en una ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguarden las copias de respaldo debe contar con los controles de seguridad física y medioambiental apropiados.

Los objetivos y responsabilidades del área de tecnología de sistemas de información específicos de este capítulo relacionado con las copias de respaldo de la información son:

- Generar y adoptar los procedimientos para la generación, restauración, almacenamiento y tratamiento para las copias de respaldo de la información, velando por su integridad y disponibilidad.
- Disponer de los recursos necesarios para permitir la identificación de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.
- Llevar a cabo los procedimientos para realizar pruebas de recuperación a las copias de respaldo, para así comprobar su integridad y posibilidad de uso en caso de ser necesario.
- Definir las condiciones de transporte o transmisión y custodia de las copias de respaldo de la información que son almacenadas externamente.
- Proporcionar apoyo para la definición de las estrategias de generación, retención y rotación de las copias de respaldo de la los activos información del H&A CONSULTING LTDA.

Responsabilidades de los usuarios:

- Es responsabilidad de los usuarios de la plataforma tecnológica del H&A CONSULTING LTDA identificar la información crítica que debe ser respaldada y almacenarla de acuerdo con su nivel de clasificación.

Monitoreo:

El área de tecnología de sistemas de información sin previo aviso puede realizar brigadas de monitoreo para verificar el estado de las copias de respaldo de la información y generar el respectivo informe de lo encontrado.

LINEAMIENTO 10: GESTIÓN DE VULNERABILIDADES

H&A CONSULTING LTDA a través de el área de tecnología de sistemas de información revisará periódicamente la aparición de vulnerabilidades técnicas sobre los recursos de la plataforma tecnológica por medio de la realización periódica de pruebas de vulnerabilidades, con el objetivo de realizar la corrección sobre los hallazgos arrojados por dichas pruebas.
Los objetivos y responsabilidades del área de tecnología de sistemas de información específicos de este capítulo relacionado con la gestión de vulnerabilidades son:

- Revisar periódicamente la aparición de nuevas vulnerabilidades técnicas y reportarlas a los desarrolladores de los sistemas de información, con el fin de prevenir la exposición al riesgo de estos.
- Generar y ejecutar o monitorear planes de acción para la mitigación de las vulnerabilidades técnicas detectadas en la plataforma tecnológica.
- Revisar, valorar y gestionar las vulnerabilidades técnicas encontradas, apoyándose en herramientas tecnológicas para su identificación.

Monitoreo:

El área de tecnología de sistemas de información sin previo aviso puede realizar brigadas de monitoreo para verificar el estado de la plataforma tecnológica con el fin de encontrar la aparición de nuevas vulnerabilidades técnicas y generar el respectivo informe de lo encontrado.