RHEMA
INTERNACIONAL

MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

RHEMA
INTERNACIONAL

MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. INTRODUCCION

El manual de Políticas de Seguridad de la Información establece los lineamientos y políticas administrativas, técnicas y legales, las cuales deben ser adoptadas todos los trabajadores, contratistas, proveedores, y todo personal externo que utilice los servicios de tecnologías de la información de RHEMA INTERNACIONAL.

Las políticas de seguridad descritas se encuentran enfocadas al cumplimiento de la normatividad legal colombiana vigente y a las buenas prácticas de seguridad de la información, basadas en la norma ISO 27001/2013 y al modelo de seguridad y privacidad de la información del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia.

2. OBJETIVO

El objetivo del presente documento es establecer las políticas en seguridad de la información de RHEMA INTERNACIONAL, con el fin de regular la gestión de la seguridad de la información, asegurando el cumplimiento de los principios de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información

3. ALCANCE

Comprende el cumplimiento de los estándares de seguridad bajo las normas de sistema de gestión seguridad informática SGSI ISO 27001, los requerimientos establecidos de seguridad por MINTIC y legislación vigente.

Las Políticas de Seguridad de la Información son aplicables para todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, trabajadores, contratistas y proveedores que presten sus servicios o tengan algún tipo de vinculación con RHEMA INTERNACIONAL, para el adecuado cumplimiento de sus funciones y para conseguir un adecuado nivel de seguridad y protección de los activos de información.

Debe ser conocida y de obligatorio cumplimiento por parte de trabajadores, contratistas y terceros que acceden al uso al uso de las plataformas y servicios tecnológicos que preste la Empresa

4. MARCO LEGAL

TIPO	No.	TEMA	FECHA	ORIGEN		
				Nacional	Distrital	Interna
Ley	1273	Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"· y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".	2009	X		

Decreto	235, Art.1-4	Por el cual se regula el intercambio de información entre Empresas para el cumplimiento de funciones pública	2010	X		
Ley	1581	Por el cual se dictan disposiciones generales para la protección de datos personales.	2012	X		
Decreto	1377	Tiene como objeto reglamentar parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.	2013	X		
Ley	1712	Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.	2014	X		
Decreto	2573	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones	2014	X		
Decreto	1074	Por el cual Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo.	2015	X		
Decreto	415	Por el cual se adiciona el Decreto único Reglamentario del sector de la Función Pública, decreto número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de información y las comunicaciones.	2016	X		
Decreto	1008	"Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones	2018	X		
Ley	1928	"Por medio de la cual se aprueba el «convenio sobre la ciberdelincuencia», adoptado el 23 de noviembre de 2001, en Budapest.	2018	X		

5. DOCUMENTOS DE REFENCIA

TIPO DOCUMENTO	DESCRIPCIÓN DEL DOCUMENTO
Modelo de Seguridad y Privacidad de la Información	Recopilación de las mejores prácticas, nacionales e internacionales, para suministrar requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad y Privacidad de la Información del El Ministerio de Tecnologías de la Información y las Comunicaciones
Norma Técnica Internacional ISO 27001, 27002, 27005,27031	Norma internacional emitida por la Organización Internacional de Normalización (ISO) para gestionar la seguridad de la información.

6. TERMINOS Y DEFINICIONES

Activo: Se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

Amenaza: situaciones que desencadenan en un incidente en la Empresa, realizando un daño material o pérdidas inmateriales de sus activos de información

Análisis de riesgos: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Áreas seguras: Lugares donde se encuentra localizada la información crítica para la organización, éstas estarán protegidas por un perímetro de seguridad y por los controles de acceso pertinentes.

Back-up (copia de respaldo): Copia de seguridad de los archivos, aplicaciones y/o bases de datos disponibles en un soporte magnético (generalmente discos o CDs), con el fin de poder recuperar la información en caso de un daño, borrado accidental o un accidente imprevisto.

Base de datos: Conjunto de archivos de datos recopilados, definidos, estructurados y organizados con el objeto de brindar información.

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

Cortafuegos: (firewall en inglés) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Contraseña: Cadena de caracteres que permite validar la autenticidad de una cuenta de usuario.

Cuenta de Usuario: Credencial que identifica a un usuario para autenticarse sobre una plataforma tecnológica.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una empresa autorizada.

Evaluación del riesgo: Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

Evento de seguridad de la información: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

Gestión del riesgo: actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.

Incidente de seguridad de la información: un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos

Niveles de respaldo de información: Hace referencia a los diferentes ambientes en los cuales la copia de seguridad se guarda de manera oportuna con el fin de tener varios niveles de recuperación de la información en caso de desastre.

No repudio: El no repudio o irrenunciabilidad es un servicio de seguridad que permite probar la participación de las partes en una comunicación.

Plan de Contingencia: Procedimientos alternativos de una Empresa cuyo fin es permitir el normal funcionamiento de esta y/o garantizar la continuidad de las operaciones, aun cuando algunas de sus funciones se vean afectadas por un accidente interno o externo.

Plataforma Tecnológica: Una plataforma tecnológica es una agrupación de equipamientos técnicos y humanos destinados a ofrecer unos recursos tecnológicos para la realización de las tareas de los usuarios

Política: Instrucciones mandatarias que indican la intención y la directriz de la alta gerencia respecto a la operación de la Empresa.

Política de escritorio despejado: La política de la empresa que indica a los empleados que deben dejar su área de trabajo libre de cualquier tipo de informaciones susceptibles de mal uso en su ausencia.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Riesgo residual: nivel restante de riesgo después del tratamiento del riesgo.

Seguridad de la información: preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad.

Servidor: En redes locales se entiende como el software que configura un PC u otro computador como servidor para facilitar el acceso a la red y sus recursos.

Sistema de gestión de la seguridad de la información - SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de

seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

Software Antivirus: Herramienta cuyo objetivo es detectar y eliminar virus informáticos.

TI: se refiere a tecnologías de la información

TIC: se refiere a tecnologías de la información y comunicaciones

Tratamiento del riesgo: proceso de selección e implementación de medidas para modificar el riesgo.

Valoración del riesgo: proceso global de análisis y evaluación del riesgo

Virus: Son programas creados para infectar sistemas y otros programas creándoles modificaciones y daños que hacen que estos funcionen incorrectamente.

Vulnerabilidad: debilidad de un activo o grupo de activos, que puede ser aprovechada por una o más amenazas. Potencialidad o la posibilidad de que se materialice una amenaza sobre el activo de información.

7. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACION

La información de la empresa se considera como uno de los principales activos de la Empresa, y como tal, debe ser protegida adecuadamente con controles administrativos, técnicos y legales de forma que se evite que persona o medio físico no autorizado pueda acceder, operar, distribuir la información, atento contra la integridad, confidencialidad y disponibilidad de los activos de información.

RHEMA INTERNACIONAL SAS orienta sus esfuerzos a la preservación de la confidencialidad, integridad, disponibilidad, a la continuidad de las operaciones de gobernabilidad, la administración y/o gestión de riesgos, la creación de cultura y conciencia de seguridad en los trabajadores, contratistas, proveedores y personas que hagan uso de los servicios de tecnologías de la información y de los activos de información de la Empresa, tomando como base que la efectividad de esta política depende finalmente del comportamiento de los usuarios y del cumplimiento de los controles establecidos en las políticas de seguridad descritas en el presente documento, fundamentados en la norma técnica colombiana NTC-ISO-27001:2013 y el modelo de seguridad y privacidad de la información de MINTIC.

8. POLITICAS SEGURIDAD DE LA INFORMACIÓN

8.1. Políticas Generales

8.1.1. El proceso de IT es el único facultado para administrar y configurar el acceso a los recursos de la plataforma tecnológica en la empresa de acuerdo con la descripción de cargo.

8.1.2. El manejo de la información y los servicios en la nube están autorizados siempre y cuando se cumpla con los acuerdos de confidencialidad, integridad y disponibilidad, además, que exista un contrato de servicio y el proveedor cumpla con los requerimientos de las normas y legislaciones vigentes.

8.1.3. Para el formato de Perfil de seguridad se identifica por cargos los controles de acceso, el software autorizado, los permisos de los productos corporativos y no corporativos, el nivel de acceso a internet, los permisos sobre medios removibles, acceso a los tipos de información y acceso múltiple factor de autenticación

8.1.4. Se retira y se da de baja aquellos equipos (servidores, desktop o portátiles) que, por sus características técnicas, software base, soporte han cumplido su vida útil y son punto vulnerable de seguridad.

8.1.5. Para la asignación de privilegios de personal nuevo, su acceso estará sujeto a la aprobación y solicitud del jefe inmediato; y autorización de dirección administrativa para su gestión.

8.1.6. Se realiza un monitoreo diario y constante del estado operativo de la red y la disponibilidad de la información

8.2. Políticas de Internet.

8.2.1. El uso de internet es únicamente para actividades relacionadas con las funciones del negocio, manteniéndose las restricciones de seguridad establecidas por la empresa.

8.2.2. El uso de servicios de mensajería instantánea solo se utilizará para actividades de la empresa y el acceso a las redes sociales estará autorizado solo a un grupo restringido de usuarios teniendo en cuenta su perfil.

8.2.3. Solo se permite el acceso a la red de internet corporativa a los equipos que están en el inventario de activos.

8.2.4. Para clientes, visitantes como aliados estratégicos, consultores, freelance y proveedores, se le habilitará el acceso a la red pública de internet alterna la cual no tendrá ningún tipo de relación con la red interna de RHEMA INTERNACIONAL.

8.2.5. No se permite el uso de los recursos de internet corporativo para la descarga, distribución y/o reproducción de música, videos y similares.

8.3. Políticas Base de Datos.

8.3.1. Se realizan planes de mantenimiento de la información de tal modo que las bases de datos de producción tienen un tamaño menor a 500 GB.

8.3.2. Una vez cumplido este tiempo se deberá hacer entrega al cliente mediante acta y posteriormente eliminación dejando acta firmada.

8.4. Políticas de BACKUP.

8.4.1. Los trabajadores son responsables de mantener la información correspondiente al área y a la gestión de sus colaboradores en el servidor principal.

8.4.2. Para los cargos de la alta dirección, se realizará las copias de seguridad de manera automática.

8.4.3. De presentarse un evento de seguridad de la información o falla física del equipo de cómputo el área de TI restaurara la conexión que el usuario tiene con el servidor principal, los archivos que el funcionario pudiera tener en el equipo no deben generar traumatismos para la continuidad de su cargo ya que estos no pueden ser recuperados.

8.4.4. Bajo ninguna eventualidad ni solicitud se entregará copia de las bases de datos y servidores en dispositivos como discos duros externos, USB, CD, DVD. Salvo por la solicitud escrita del cliente y la aprobación de gerencia.

8.4.5. El área de TI garantiza los respaldos de información que reposa en los ambientes productivos de la empresa RHEMA INTERNACIONAL SAS los cuales están debidamente informados a la gerencia.

8.4.6. Se realiza un backup diario full de la información contenida en el servidor principal en la herramienta de backup de la empresa.

8.4.7. El backup generado del servidor principal, se almacena en una unidades locales y externas de almacenamiento debidamente cifrado.

8.4.8. Para el retiro de un funcionario de la empresa se realiza un backup de la información por parte del área de TI tan pronto se reciba el portátil o equipo asignado por la empresa. Además, se realiza la cancelación de la cuenta de acceso a los servicios compartidos

8.5. Política Acceso Físico.

8.5.1. El acceso al cuarto de sistemas está restringido únicamente al personal autorizado y bajo la supervisión del área de TI con previa aprobación de ingeniero de sistemas.

8.5.2. Para el monitoreo de las instalaciones, se cuenta con un circuito cerrado de televisión, con un periodo de conservación de la información de mínimo 7 días.

8.5.3. Para los visitantes, el funcionario que autoriza su ingreso lo acompaña de manera permanente mientras permanezca dentro de las instalaciones de la empresa.

8.5.4. Para acceso a las áreas seguras se cuenta con un dispositivo de control de acceso con huella donde quedan registrado el ingreso de los trabajadores de la empresa.

8.6. Política Acceso remoto

8.6.1. El acceso remoto a los servidores críticos y bases de datos, se realizan por el líder, administrador de TI.

8.6.2. El acceso remoto a la información corporativa solo está autorizado vía VPN debidamente autorizado por la gerente administrativa

8.6.3. Se debe tener implementado como múltiple factor de autenticación aplicaciones del dispositivo Mobile o de terceros mediante la cual se accederá a la plataforma tecnológica de la RHEMA INTERNACIONAL SAS.

8.6.4. Se establece el tiempo de desconexión por inactividad de la sesión es de 10 minutos.

8.6.5. El gerente administrativo autoriza los accesos remotos de los empleados y proveedores.

8.6.6. Está prohibido copiar, mover o almacenar información de las bases de datos de los servidores cuando se acceda mediante tecnologías de acceso remoto.

8.7. Política Acceso inalámbrico.

8.7.1. Los puntos de acceso inalámbrico autorizados por la empresa son la red identificada como RHEMA202 los trabajadores de RHEMA INTERNACIONAL SAS y la red identificada como RHEMA INVITADOS para los usuarios externos.

8.7.2. No está permitido la utilización y conexión de la red inalámbrica de la empresa para a actividad diferente a la labor del empleado (se aplica la Políticas de Internet).

8.8. Política Acceso múltiple factor de autenticación.

8.8.1. El acceso a los servidores y base de datos se realizará a través múltiple factor de autenticación, por previa autorización del oficial de seguridad.

8.8.2. Está prohibido copiar, mover o almacenar datos en discos duros locales, dispositivos electrónicos extraíbles al acceder con tecnologías de acceso remoto.

8.9. Política Dispositivos móviles.

8.9.1. Los dispositivos móviles autorizados a conectarse a la red inalámbrica corporativa (WLAN) son los portátiles que hacen parte del inventario de activos o equipos propios de la alta dirección.

8.9.2. Los dispositivos móviles autorizados para contener, administrar o manejar información privada y/o confidencial de la empresa son de propiedad de la RHEMA INTERNACIONAL SAS

8.9.3. El funcionario al cual se le asigna el equipo móvil es responsable por su seguridad y correcta operación dentro de la red interna y en lugares públicos.

8.9.4. Los dispositivos móviles personales de los visitantes o trabajadores que requieran tener acceso a una red principal para el acceso a la red pública de internet deben solicitar a la coordinación administrativa.

8.10. Política Trabajadores

8.10.1. Se debe retirar inmediatamente cualquier documento enviado a las impresoras que contenga información sensible, secreta o confidencial.

8.10.2. Los documentos electrónicos o físicos que contienen información sensible, secreta, privada o confidencial se guardaran en condiciones de seguridad y con acceso de lectura por personal autorizado.

8.10.3. Los trabajadores de la empresa son responsables del cumplimiento de las políticas de seguridad de acuerdo con el alcance que se define en este documento.

8.10.4. En ninguna circunstancia el trabajador gestionara información o procesos de su cargo en un equipo diferente del corporativo asignado por Rhema

8.11. Política de Mejora Continua

8.11.1. De acuerdo con las auditorías realizadas, la empresa deberá realizar actividades para controlar y corregir los hallazgos o no conformidades presentadas.

8.11.2. Se debe evaluar y revisar los hallazgos o no conformidades desde la causa del problema con el fin de mitigarlo

8.11.3. Se debe revisar las lecciones aprendidas con el fin de que no se repita las no conformidades encontradas.

8.11.4. Generar e implementar tareas o actividades, relacionadas con un ticket para llevar el seguimiento en las siguientes auditorias.

8.12. Política Uso Compartidos en la Red (Carpetas)

8.12.1. Se prohíbe almacenar o intercambiar archivos de audio en cualquier formato (WAV, Mp3, etc.) para fines personales.
8.12.2. Se prohíbe almacenar o intercambiar archivos de videos y/o fotografías personales en cualquier formato.
8.12.3. Se prohíbe guardar archivos que no sean de uso laboral.
8.12.4. Antes de eliminar cualquier información del recurso compartido, verifique con el administrador o propietario de la información que esta va a ser borrada.
8.12.5. Se debe guardar únicamente información que se está trabajando.
8.12.6. El usuario de la unidad del recurso compartido debe reportar al jefe inmediato si encuentra información que no es de su área.
8.12.7. Si en las carpetas se encuentran archivos de música, fotos, videos, etc. de carácter personal, estos serán borrados inmediatamente sin notificarle al usuario.
8.12.8. El tiempo de retención de la información es de 1 mes, una vez transcurrido este tiempo se realiza depuración de la información.
8.12.9. El no cumplimiento de esta política atenta contra la seguridad de la información y es sancionado de acuerdo con el procedimiento definido.

8.13. Política Escritorio Limpio

8.13.1. Ejecutar el bloqueo de pantalla siempre que el responsable o usuario del equipo se ausente de la terminal, ejecutando la combinación de teclas Windows (⊞) + L.
8.13.2. Cerrar sesiones de usuario cuando no se requiera los servicios del equipo durante tiempos superiores a 5 minutos.
8.13.3. En caso de usar medios físicos de autenticación tipo tokens o tarjetas inteligentes se deberá definir en las políticas de la maquina o de dominio el bloqueo de la estación al retirar el medio físico.
8.13.4. Ejecutar el procedimiento de clasificación, etiquetado y manejo de la información de forma segura y ordenada en rutas de acceso recordables.
8.13.5. En la pantalla no debe permanecer ningún icono, acceso directo o archivo, esta debe estar completamente despejada.
8.13.6. Para el personal operativo en la pantalla solo deben permanecer los iconos de acceso directo a las diferentes herramientas de gestión de la solución, no deben permanecer archivos digitales de ningún tipo.

8.14. Política de Seguridad en la Nube

8.14.1. Realizar monitoreo a los registros de trasferencia de datos hacia la nube.
8.14.2. Implementar controles de criptografía para la transferencia de información.
8.14.3. Proteger los volúmenes de su exposición a un clonado mediante snapshot.
8.14.4. Realizar backup de la información que se envía hacia la nube

8.15. Política Gestión del Incidente

8.15.1. Se define roles y responsabilidades dentro de la empresa para evaluar los riesgos y así mantener la operación, la continuidad y la disponibilidad del servicio.
8.15.2. Gestionar los eventos de seguridad de la información para detectar e identificar si es necesario o no clasificarlos como incidentes de seguridad de la información.
8.15.3. Definir de manera oportuna los eventos de seguridad de la información para ser evaluados y dar respuesta de la manera más eficiente y adecuada.
8.15.4. Asegurar las lecciones aprendidas que dejan los incidentes de seguridad de la información y su gestión para aprender rápidamente. Con el fin de mejorar el esquema global de la gestión de incidentes de seguridad de la información.
8.15.5. Definir los mecanismos que permitan cuantificar y monitorear los tipos, volúmenes y costos de los incidentes de seguridad de la información, a través de una base de conocimiento y registro de incidentes y a través de los indicadores del sistema de gestión de seguridad de la información.
8.15.6. Definir los procedimientos formales de reporte y escalada de los incidentes de seguridad.
8.15.7. Establecer variables de posible riesgo, en efecto, es la posible valoración de aspectos sensibles en los sistemas de información.

8.16. Política de Equipo de computo

8.16.1. Se asignará equipo de cómputo al empleado en caso de ser necesario
8.16.2. Las funciones del cargo se deben gestionar en dispositivos corporativos asignados

9. SANCIONES A LAS VIOLACIONES DE LA POLITICA DE SEGURIDAD DE LA INFORMACIÓN

El área de TI solicitará la publicación en la Intranet el documento Políticas de Seguridad de la Información, socializará su contenido y hará cumplir su alcance. El desconocimiento de la política de seguridad de la información de RHEMA INTERNACIONAL SAS, por parte de trabajadores, contratistas y terceros puede generar acciones disciplinarias. Las investigaciones disciplinarias y las respectivas sanciones le corresponden a la Dirección de Gestión Corporativa y Control Interno Disciplinario.

Actuaciones que con llevan a la violación de la seguridad de la información establecida por la secretaria Distrital de Desarrollo Económico:

9.1. No reportar los incidentes de seguridad o las violaciones a las políticas de seguridad, cuando se tenga conocimiento de ello.
9.2. No actualizar la información de los activos de información a su cargo.
9.3. Clasificar y registrar de manera inadecuada la información, desconociendo los estándares establecidos para este fin.
9.4. No guardar de forma segura la información cuando se ausenta de su puesto de trabajo o al terminar la jornada laboral, de documentos impresos que contengan información pública reservada, información pública clasificada (privada o semiprivada).
9.5. No guardar la información digital, producto del procesamiento de la información perteneciente a la Empresa.
9.6. Dejar información pública reservada, en carpetas compartidas o en lugares distintos al servidor de archivos, obviando las medidas de seguridad.
9.7. Dejar las gavetas abiertas o con las llaves puestas en los escritorios,

9.8. Dejar los computadores encendidos en horas no laborables.
9.9. Permitir que personas ajenas a la Empresa, deambulen sin acompañamiento, al interior de las instalaciones, en áreas no destinadas al público.
9.10. Almacenar la información de la Empresa en los computadores personales de los usuarios,
9.11. Solicitar cambio de contraseña de otro usuario, sin la debida autorización del titular o su jefe inmediato.
9.12. Hacer uso de la red de datos de la Empresa, para obtener, mantener o difundir material pornográfico u ofensivo, cadenas de correos y correos masivos no autorizados.
9.13. Utilización de software no relacionados con la actividad laboral y que pueda degradar el desempeño de la plataforma tecnologías de la Información de la Empresa.
9.14. Enviar sin autorización información de la Empresa a través de correos electrónicos personales.
9.15. Enviar información pública reservada o información pública clasificada por correo, copia impresa o electrónica sin la debida autorización y sin la utilización de los protocolos establecidos para la divulgación.
9.16. Usar dispositivos de almacenamiento externo en los computadores sin la autorización previa.
9.17. Permitir el acceso de trabajadores a la red corporativa, sin la autorización previa.
9.18. Negligencia en el cuidado de los equipos, dispositivos portátiles o móviles entregados para actividades propias de la Empresa.
9.19. No cumplir con las actividades designadas para la protección de los activos de información de la Empresa.
9.20. Descuidar documentación con información crítica, reservada o clasificada de la Empresa, sin las medidas apropiadas de seguridad que garanticen su protección.
9.21. Almacenar información crítica reservada o clasificada, en cualquier dispositivo de almacenamiento que no permanezca a Empresa o conectar computadores portátiles u otros sistemas eléctricos o electrónicos personales a la red de datos de la Empresa sin la debida autorización.
9.22. Promoción o mantenimiento de negocios personales, o utilización de los recursos tecnológicos de la Empresa para beneficio personal.
9.23. El que sin autorización acceda en todo o parte de la infraestructura informática o se mantenga dentro del mismo en contra de la voluntad de la Empresa.
9.24. El que impida u obstaculice el funcionamiento o el acceso normal a la infraestructura informática, los datos informáticos o las redes de telecomunicaciones de la Empresa, sin estar autorizado.
9.25. El que destruya, dañe, borre, deteriore o suprima datos informáticos o un sistema de tratamiento de información de la Empresa.
9.26. El que distribuya, envíe, introduzca software malicioso u otros programas de software con efectos dañinos en la plataforma tecnológica de la Empresa.
9.27. El que modifique, altere datos personales de las bases de datos de la Empresa sin la debida autorización.
9.28. El que superando las medidas de seguridad de la información suplante un usuario ante los sistemas de autenticación y autorización establecidos por la Empresa.
9.29. No mantener la confidencialidad de las contraseñas de acceso a la red de datos, los recursos tecnológicos o los sistemas de información de la Empresa o permitir que otras personas accedan con el usuario y clave del titular a éstos.

9.30. Permitir el acceso u otorgar privilegios de acceso a las redes de datos de la Empresa a personas no autorizadas.

9.31. Llevar a cabo actividades fraudulentas o ilegales, o intentar acceso no autorizado a la infraestructura de tecnologías de las Información de la Empresa.

9.32. Ejecutar acciones tendientes a eludir o variar los controles establecidos por la Empresa.

9.33. Retirar de las instalaciones de la Empresa equipos de cómputo que contengan información institucional sin la debida autorización.

9.34. Sustraer de las instalaciones de la Empresa, documentos con información institucional calificada como información pública reservada o clasificada, o abandonarlos en lugares públicos o de fácil acceso.

9.35. Entregar, enseñar y divulgar información institucional, calificada como información pública reservada y clasificada a personas o Empresa es no autorizadas.

9.36. Ejecución de cualquier acción que pretenda difamar, abusar, afectar la reputación o presentar una mala imagen de la Empresa, trabajadores o contratistas.

9.37. Realizar cambios no autorizados en la plataforma tecnológica de la Empresa.

9.38. Acceder, almacenar o distribuir pornografía infantil.

9.39. Instalar programas o software no autorizados en los equipos de cómputo, cuyo uso no esté autorizado por la Subdirección de Tecnología y Sistemas la Empresa.

9.40. Copiar sin autorización las aplicaciones de software de la Empresa, o violar los derechos de autor o acuerdos de licenciamiento.

10. ACUERDO DE CONFIDENCIALIDAD

Todos los trabajadores y contratistas deben firmar la cláusula y/o acuerdo de confidencialidad que deberá ser parte integral de los contratos laborales y de prestación de servicios utilizando términos legalmente ejecutables y contemplando factores como responsabilidades y acciones de los firmantes para evitar la divulgación de información no autorizada. Este requerimiento también se aplicará para los casos de contratación temporal o cuando se permita el acceso a información y/o a los recursos a personas o Empresas externas.

Víctor Manuel Nieto Gómez

Gerente General

Versión: 0 - 21/02/2024
Revisión: 07/02/2025
Código: DE-PO-011