MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

SIG
SISTEMA INTEGRADO DE GESTIÓN

Código MA-5.5-02 Versión 01

NIVEL 1:	NIVEL 2:
5.0 PROCESO DE GESTIÓN DE RECURSOS	5.5 Gestión de Tecnología de la Información

ELABORÓ:	REVISÓ:	APROBÓ:
Fecha: 2023-02-13 Coordinador Gestión T.I Consultor externo SIG Profesional del Sistema de Gestión	Fecha: 2023-02-13 Coordinador Gestión T.I	Fecha: 2023-02-28 Director Administrativo y Financiero

TABLA DE CONTENIDO

1. OBJETO Y CAMPO DE APLICACIÓN

Definir las políticas de seguridad de la información, controles y prácticas de ONAC, con el propósito de asegurar su confidencialidad, integridad y disponibilidad de la información y la protección de los activos de información de acuerdo con los requisitos del negocio, reglamentos y leyes pertinentes.

2. ALCANCE

Este documento aplica los empleados, proveedores, contratistas y visitantes de ONAC, con acceso a la información y a los sistemas de procesamiento de la información.

Esta política incluye disposiciones sobre el uso aceptable de los activos de información, incluyendo los equipos (servidores, estaciones de trabajo, equipos móviles, equipos de comunicaciones e infraestructura tecnológica), los servicios (internet, intranet, correo electrónico, VPN y aplicaciones corporativas), el software y la información (archivos, documentos y bases de datos) que apoyan los procesos de ONAC.

Los controles definidos están dirigidos a todas las personas naturales y jurídicas que tengan una vinculación con ONAC (laboral, contractual, orden de servicio, cliente, asociados, demás partes interesadas) y que tengan acceso a su información, por lo tanto, es su responsabilidad conocer y aceptar los presentes términos y condiciones para comprometerse a dar buen uso de los recursos de información físicos, lógicos y de los activos que los procesan.

Igualmente, este documento se aplica a los procesos de tratamiento y custodia de la información, entre los que se encuentran el registro, el almacenamiento, la clasificación, la consulta y la disposición final.

3. REFERENCIAS NORMATIVAS

Los siguientes documentos normativos, de requisitos o lineamientos, son aplicables al sistema integrado de gestión de ONAC, en su versión citada:

- ISO 27000:2014 Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información — Visión general y vocabulario
- ISO 27001:2013 Sistemas de gestión de seguridad de la información — Requisitos
- ISO 27002:2013 Tecnología de la información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información.
- ISO 22301:2019 Sistemas de gestión de continuidad del negocio — Requisitos.

4. TÉRMINOS Y DEFINICIONES

Para fines de este documento se aplican los términos y definiciones incluidos en los documentos de definición y referencia, en especial:

Seguridad de la información: Preservar la ***disponibilidad, integridad y confidencialidad*** de la información y de los servicios de procesamiento de la información.

- **Disponibilidad:** Que la información se encuentre al acceso de quien la necesite en los procesos del negocio
- **Integridad:** Preservar la exactitud y estado de la información, previniendo su daño o deterioro
- **Confidencialidad:** propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Información: conjunto de datos organizados y procesados que crean mensajes, instrucciones, operaciones, funciones y cualquier otro tipo de actividad que genera valor y conocimiento a una organización.

Políticas de seguridad de la información: Intenciones y directrices de una organización en materia de seguridad de la información, expresadas formalmente por las Alta Dirección.

Transferencia de información: implica el envío de información hacia un destinatario, el cual asumirá las obligaciones de responsable del tratamiento de esta información.

Usuario de la información: son los clientes, empleados, contratistas, proveedores, asociados y otros públicos de interés que tiene acceso a información del Organismos Nacional de Acreditación de Colombia - ONAC.

Medios removibles: objeto dispuesto para el almacenamiento de información que permite su posterior consulta.

Respaldo de información: copia de información realizada a los datos originales que se realiza con el fin de disponer de un medio para su posterior recuperación en caso de pérdida o daño.

La ingeniería social: Es el conjunto de técnicas que usan los cibercriminales para engañar a los usuarios incautos para que les envíen datos confidenciales, infecten sus equipos con malware o abran enlaces a sitios infectados.

Log: Registro oficial de eventos durante un rango de tiempo en particular. Se usa para registrar datos o información sobre quién, qué, cuándo, dónde y por qué un evento ocurre para un dispositivo en particular o aplicación.

Token: Es un dispositivo que genera códigos de acceso que se le da a un usuario autorizado de un servicio computarizado para facilitar el proceso de autenticación.

5. PARTICIPANTES Y RESPONSABILIDADES

Director Ejecutivo	• Aprobar las políticas y controles y disposiciones definidas en este manual.
Director Administrativo y Financiero	• Validar los lineamientos definidos de este documento y sus modificaciones. • Asegurar la disponibilidad de los recursos financieros, para ejecutar las actividades que surjan para el mantenimiento y disposiciones definidas en este manual.
Coordinador de Gestión de TI	• Revisar, proponer y estructurar los controles que en materia de seguridad de la información requieren ser mantenidas en ONAC. • Garantizar el seguimiento y los controles para la aplicación e implementación de los lineamientos definidos en el presente manual. • Asegurar el adecuado tratamiento y cuidado de los datos e información contenida en las bases de datos de los sistemas de información de ONAC. • Identificar los riesgos y controles necesarios para gestionar la Seguridad de la Información en ONAC. • Gestionar el presupuesto aprobado y asignado para el cumplimiento de la gestión de la seguridad de la información.
Coordinador de Gestión Documental	• Asegurar que los controles establecidos para la seguridad de los documentos físicos que están bajo su responsabilidad se cumplan.
Coordinador del Sistema de Gestión/ Profesional del Sistema de Gestión	• Garantizar que el contenido de este manual se ajuste a los requisitos de la documentación del Sistema de Gestión.
Directores, jefes y Coordinadores	• Clasificar la información para definir los permisos de acceso por parte del personal, de acuerdo con sus funciones y competencias. • Garantizar que la matriz de activos fijos de información permanezca actualiza. • Mantener la integridad, confidencialidad y disponibilidad del activo de información, durante su utilización, administración, custodia y disposición final. • Proponer las acciones requeridas que garanticen el adecuado manejo y seguridad de la información en ONAC. • Participar en la identificación y análisis de los riesgos y controles asociadas al manejo de la información a su cargo. • Garantizar que los controles establecidos para la seguridad de los documentos que están bajo su responsabilidad se cumplan. • Informar al área jurídica de ONAC la información y datos necesario para transmitir información requerida por entes de control y vigilancia.
Personal interno	• Dar cumplimiento a los controles establecidos para la seguridad de la información que están bajo su responsabilidad.
Personal externo	• Dar cumplimiento a los controles establecidos para la seguridad de la información que están bajo su responsabilidad.
Todo el personal	• Notificar oportunidades de mejora para la gestión de la seguridad de la información.

6. INTRODUCCIÓN

En toda la información del Organismo Nacional de Acreditación de Colombia -ONAC, está representado en el conocimiento, los datos y documentos que como consecuencia resultan del mismo. Su adecuado almacenamiento, tratamiento y uso permiten asegurar la estabilidad, continuidad y seguridad en las operaciones del organismo.

Con el Manual de Políticas de Seguridad de la Información se busca asegurar la estabilidad de las operaciones de ONAC desde el ámbito de la protección de la información, mediante el establecimiento de una serie de lineamientos que faciliten un abordaje sistémico del manejo de los datos y en general, del desarrollo de los procesos propios de la actividad de ONAC. Estos lineamientos establecen las líneas de acción para mitigar los diversos riesgos a los que está expuesta una organización que administra altos volúmenes de información, teniendo en cuenta la clasificación de esta, su forma de almacenamiento y transmisión.

En este mismo sentido, se busca promover en ONAC una cultura orientada a la protección y seguridad de los datos, con un enfoque basado en la mejora continua de las actividades asociadas a la gestión de riesgos por pérdida, robo o fugas de información, así como, a la vulnerabilidad en la cadena de custodia de los datos.

Por ello, los lineamientos y disposiciones contenidos en este manual son de obligatorio cumplimiento por parte del personal vinculado a ONAC, ya sea a través de un contrato laboral, de prestación de servicios o de una orden de servicio.

6.1 Política de seguridad de la información

La alta dirección del Organismo Nacional de Acreditación de Colombia – ONAC, ha establecido la política del Sistema Integrado de Gestión. Tomando como base esta política se han establecido las siguientes directrices e intenciones en materia de seguridad de la información y la gestión de continuidad:

- Gestionar (Eliminar o mitigar) los riesgos relacionados con las actividades y procesos, y la seguridad de la información
- Asegurar la continuidad en la prestación de los servicios de acreditación
- Proteger la confidencialidad e integridad de la información de sus clientes y partes interesadas.
- Asegurar la disponibilidad de los servicios de tecnología de la información relacionados con las actividades de acreditación
- Dar cumplimiento a los requisitos legales, reglamentarios y normativos relacionados con los servicios de acreditación, la seguridad de la información y la continuidad.
- Mejorar la infraestructura tecnológica, para apoyar los procesos del sistema de gestión.
- Mejora continua de los procesos del sistema de gestión

7. GESTIÓN DE LA INFORMACIÓN

7.1 Clasificación, Almacenamiento y Administración de la Información

7.1.1 Clasificación de la información

ONAC da tratamiento a información que no en todos los casos es de su propiedad, por lo tanto, es responsable de protegerla durante su recepción, custodia y disposición final. Esto es de vital importancia para garantizar confianza y continuidad en la prestación de los servicios, además, permite establecer los parámetros para la clasificación, almacenamiento y administración de la información. A continuación, se presenta la definición de dichos parámetros para ONAC:

Clasificación de la información

Toda la información contenida en los sistemas de información de ONAC deberá ser clasificada teniendo en cuenta su nivel de sensibilidad. Se deberá contar con una metodología que permita clasificar la información y conocer su valor. Los responsables de la información serán los encargados de clasificar, proteger y autorizar el acceso a la información, por lo tanto, asumen el rol de tutores de la información y la propiedad de la misma siempre será de ONAC.

Todos los datos contenidos en los sistemas de información deberán ser clasificados dentro de las siguientes categorías:

- **Información pública:** información que puede ser divulgada sin restricción alguna y cuya circulación no implica un riesgo para ONAC, ni para las personas naturales o jurídicas que la suministran.
- **Información clasificada:** información que cuenta con algún impedimento para su divulgación por contener información sensible.
- **Información de carácter privado;** la cual es de uso exclusivo de los colaboradores de ONAC para el desarrollo de sus funciones y para el acceso por parte de terceros, se requiere la autorización del responsable de la información o de la Dirección Ejecutiva de ONAC.
- **Información reservada de carácter personal;** la cual está estrechamente ligada con los derechos fundamentales del titular y/o contemplada como tal en la ley de protección de datos. Esta información no puede ser divulgada en ninguna circunstancia

La clasificación de la información deberá ser realizada por el responsable de la misma, en conjunto Gestión Documental.

Se recomienda que el usuario que divulgue información por cualquier medio tenga en cuenta la clasificación de la misma y considere el informar el tratamiento de esta en caso de ser clasificada y reservada.

7.1.2 Almacenamiento y respaldo de la información

Información en medio físico

La información física se administra en ONAC de acuerdo con lo establecido en las tablas de retención documental y los colaboradores son los responsables de la información que manejan, por lo tanto, deberán protegerla, evitar pérdidas, accesos no autorizados y/o su utilización indebida.

Todos los medios físicos donde la información de valor, sensible y/o crítica es almacenada por periodos superiores a seis (6) meses, no deberán estar sujetos a degradación rápida o deterioro, por lo tanto, la información deberá mantenerse almacenada bajo condiciones ambientales de humedad y temperatura óptimas que permitan su conservación

Información en medio electrónico

Los siguientes aspectos deberán considerarse para gestionar el almacenamiento y respaldo de la información digital en ONAC:

- Las bases de datos usadas para el ejercicio de las actividades de acreditación que contengan información clasificada como restringida, deberán incorporarse al segmento de la red de datos corporativa.
- Luego del ingreso a las aplicaciones o sistemas de información, los datos confidenciales de autenticación no deberán almacenarse en el equipo, aunque se encuentren cifrados.
- Todo dato reservado debe contar con un proceso de respaldo periódico, un periodo de retención, fechas de modificación, fecha de caducidad y disposición final.
- Toda información administrada por ONAC deberá contar con una copia de respaldo completa y actualizada, en un sitio externo al local en donde se procesan los datos.
- Los respaldos de información que se encuentran en medio magnético deben tener un proceso de validación con el fin de garantizar que no hayan sufrido algún deterioro y que podrán ser utilizados en el momento que se requiera. Toda la información contable, de impuestos y de tipo legal, debe ser conservada de acuerdo con las normas vigentes de ley.
- El área de Gestión de T.I de ONAC será la responsable de ejecutar el proceso de restauración de los backups de información.

7.1.3 Transmisión de la información

Los siguientes aspectos deberán considerarse para gestionar el almacenamiento y trasmisión de la información:

- Toda información reservada que requiera ser remitida fuera de las instalaciones de ONAC, solamente podrá ser enviada una vez se garantice de forma segura su integridad y confidencialidad.
- Todos los mensajes de correo electrónico remitidos en formato libre de texto y que contengan información reservada debe ser almacenados en el servidor en las carpetas definidas por el remisor y/o sistema de información acorde al proceso.
- Toda transmisión de información que se encuentre en una base de datos deberá cumplir con lo establecido en la Política de Tratamiento de Datos Personales de ONAC vigente
- De conformidad con la Circular Externa No. 02 del 3 de noviembre de 2015, emitida por la Superintendencia de Industria y Comercio, y de acuerdo con el Capítulo 26 del Decreto 1074 de 2015, ONAC se encuentra debidamente inscrito en el Registro Nacional de Bases de Datos de la SIC, para lo cual el área de Gestión de T.I informara cada dos meses a la jefatura Jurica de ONAC el número de bases asociadas a sistemas de información. su alcance y número de registros para que esta información se cargue o actualice en la plataforma dispuesta por la SIC

7.1.4 Eliminación segura de la información

Los siguientes aspectos deberán considerarse para gestionar la eliminación de datos:

- La eliminación de documentos se realiza de acuerdo con el procedimiento PR-5.6-03 Organización, Archivo y Custodia de documentos físicos y electrónicos.
- La eliminación de la información que no está contenida en documentos se deberá realizar de acuerdo con las tablas de retención documental.

7.1.5 Administración de la información

Consideraciones a tener en cuenta para la administración de la información:

- Toda la información reservada debe contemplar las características de integridad, confidencialidad, disponibilidad, trazabilidad, efectividad, eficiencia y cumplimiento.
- Cualquier tipo de información interna no podrá ser transferida, intercambiada o vendida a terceros para ningún propósito diferente a los del negocio. En caso de que la información sea requerida por auditores internos o externos, la entrega de la misma deberá ser autorizada por su propietario y además contar con los respectivos acuerdos de confidencialidad debidamente firmados, previo a su uso.
- El acceso a depósitos de información (almacenamiento físico o magnético) debe restringirse únicamente al personal autorizado.
- Las aplicaciones o programas deben ser modificados únicamente por el personal autorizado por el área de gestión de TI.
- Todo software que comprometa la seguridad de los sistemas se custodiará y administrará únicamente por el personal autorizado. Además, se deberá dejar registro de su uso en medio magnético o físico
- Cuando la información reservada no esté siendo utilizada, se debe almacenar cumpliendo las medidas de seguridad que garanticen su confidencialidad e integridad.
- El acceso a la información reservada se debe otorgar únicamente a personas específicas y debidamente autorizadas según procedimientos establecidos.
- Toda divulgación de información restringida a terceras personas debe estar acompañada de un contrato o acuerdo de confidencialidad.
- Se prohíbe que la información de la empresa se manipule o se utilice con el objetivo de perjudicar a la empresa.
- Se prohíbe la utilización de la información de la empresa para lucro propio o de terceros.
- La realización de copias adicionales de información sensible deberá cumplir con los procedimientos de seguridad definidos para tal fin y contar con la autorización del propietario de los datos a ser duplicados.
- Toda información histórica almacenada debe contar con los medios, procesos y programas capaces de permitir su manipulación con las mínimas medidas de seguridad requeridas, esto teniendo en cuenta las modificaciones y actualizaciones que pueden sufrir los datos y las aplicaciones a través del tiempo.
- En cualquier momento el propietario de la información puede reclasificar el nivel de confidencialidad de la misma, lo cual debe ser informado al área de Gestión Documental, para que se realice la actualización de la tabla de retención documental y al área de Gestión de T.I, para que aplique las medidas respectivas que considere
- Son derechos de propiedad intelectual exclusiva de ONAC, todos los productos desarrollados o modificados por los colaboradores o personas contratadas por el organismo.

8. SEGURIDAD FÍSICA

8.1 Áreas seguras

El acceso físico a cualquier activo de información tangible como servidores, elementos de red, hardware, documentos y demás elementos de la infraestructura como gabinetes eléctricos, gabinetes de equipos de transmisión y gabinetes de cableado estructurado, debe estar completamente restringido (solo el personal autorizado podrá manipular estos elementos). Esto se aplica sin excepción a los activos de información del segmento de red que alojan, procesan o transportan datos de los OEC y de ONAC.

a) Niveles de protección por áreas

Según el nivel de criticidad en que se encuentre clasificada la información, se deberán definir tres zonas de seguridad y protección de información:

1. Área de Restringida: Comprende lugares donde se administra y procesa información privada y confidencial, las cuales cuentan con controles de acceso mediante tarjetas de proximidad, clave de acceso y CCTV (Circuito Cerrado de Televisión). Las áreas clasificadas en esta categoría son:

- Centro de Datos y de Monitoreo de CCTV.
- Archivo Central.

2. Área de Trabajo: Lugares donde se encuentran ubicados los puestos de trabajo del personal de ONAC y donde estén instalados o almacenados equipos y/o elementos críticos con acceso restringido bajo llave a personal autorizado. Los cuales son:

- Gabinetes o armarios asignados al área de Gestión de T.I para el almacenamiento de:
    - Hardware y software.
    - Licencias de uso.
    - Dispositivos de almacenamiento y token de firmas digitales.
    - Insumos de impresoras
- Gabinetes o armarios asignados a la Coordinación de Comunicación Organizacional para almacenar material preimpreso y POP.
- Gabinetes o armarios asignados como archivos de gestión a directores y Coordinadores.

8.2 Seguridad física

Control de acceso físico

El acceso a áreas consideradas de acceso restringido será controlado a través de mecanismos de acceso (tarjetas y claves) y vigilancia de los jefes de área, que llevarán el registro del ingreso de personal en una bitácora donde se especifique la fecha y motivo de ingreso, elementos solicitados y la firma de autorización. Con el control de acceso mediante el uso de tarjetas de proximidad se identifica a los usuarios y con ayuda del CCTV se registran las entradas y salidas, lo cual permite limitar los intentos de acceso no autorizados. Los registros de estos controles deben ser almacenados y custodiados por el área de Gestión de T.I.

Estos lugares deberán contar con señalización externa que indique la restricción de acceso e interna que enfatice temas de seguridad (zonas diferentes al Centro de Datos), las puertas deben estar siempre aseguradas y bajo el estricto control del jefe de área o responsable directo.

Personas

Toda persona que visite las oficinas de ONAC deberá registrarse en la recepción y la autorización de su ingreso se gestionará con el colaborador visitado. Para ello, se deberán solicitar los datos personales (nombres, apellidos, identificación y entidad que representa), los cuales deberán ser consignados en la bitácora de recepción.

Todos los colaboradores de ONAC deben tener especial cuidado de no permitir el ingreso de personal no autorizado a las áreas restringidas. El ingreso de personas no autorizadas únicamente podrá realizarse con el acompañamiento en todo momento, de un responsable del área.

En áreas restringidas como el Centro de Datos o instalaciones con equipos tecnológicos está prohibido comer, beber o fumar y si la persona que ingresa allí requiere realizar el registro fotográfico de cualquier labor realizada, deberá solicitar autorización al encargado del área de Gestión de T.I. Al finalizar cualquier trabajo en el Centro de Datos, el personal externo deberá asegurarse que todos sus cables estén bien instalados y ordenados, dentro de sus gabinetes, así como asegurarse que todas las puertas están cerradas y aseguradas.

8.3 Seguridad de los equipos

Equipos, puestos de trabajo y otros recursos

A través de los siguientes lineamientos, ONAC busca asegurar la seguridad de la información en equipos, puestos de trabajo y demás recursos similares:

- Todo equipo informático que procese información o tenga alguna conexión con los sistemas de información de ONAC (propio o de terceros), debe cumplir con las normas de seguridad física mínimas requeridas, para evitar el acceso de personal no autorizado a los mismos.
- Los computadores, notebooks, equipos de comunicaciones, teléfonos y demás equipos de ONAC, no deben moverse, reubicarse o ser sacados de las instalaciones sin la respectiva autorización (por correo electrónico) del jefe directo o del responsable del área de Gestión de T.I.
- Los servidores de datos, los equipos de comunicación y los servidores de aplicaciones estarán ubicados en lugares seguros, de acuerdo con lo establecido en las normas en las que se basan los lineamientos aquí definidos.
- Los documentos en donde se encuentre información clave para los sistemas de información como; direcciones IP internas, configuraciones, información de los sistemas de comunicación y computo, entre otros, son de carácter privado y deben ser custodiados por el Área de Gestión de T.I y la Dirección Administrativa y Financiera.
- El Centro de Datos, los gabinetes y armarios en donde se almacenan las cintas, discos y documentos con información de ONAC, serán de acceso restringido y controlado mediante cerraduras, tarjetas de proximidad calve de acceso o lector biométrico.
- Ninguna estación de trabajo, notebook o dispositivo móvil podrá ser conectado a la red interna sin antes ser verificado y autorizado por el área de Gestión de T.I. Los puntos de conexión de red no utilizados no tendrán cables de red conectados para su uso a excepción de los disponibles en las salas de juntas.
- Los tomacorrientes que se encuentran en el Centro de Datos no se podrán utilizar libremente, esto con el fin de evitar incidentes que puedan afectar los servidores y equipos instalados en este lugar, y en caso de que se requiera, el encargado del área de Gestión de T.I, será el responsable de indicar en qué lugares se puede realizar dicha conexión.
- No se instalarán líneas telefónicas, canales de transmisión de datos, módems o se realizarán cambios en la configuración de los equipos instalados sin la autorización correspondiente del área de Gestión de T.I.
- No se deberá anunciar en las carteleras públicas de ONAC, información sobre la ubicación de sitios de alta seguridad.

8.4 Requisitos de Seguridad para estaciones de trabajo

Para proteger la integridad y el manejo seguro de estaciones de trabajo se debe cumplir las siguientes reglas de uso:

- El equipo debe instalarse únicamente por el personal de sistemas o por el proveedor.
- El equipo debe identificarse adecuadamente según el PR-5.5-01 Gestión de activos de Información y licenciamiento de forma visible y clara para prevenir hurto y facilitar la trazabilidad.
- Se prohíbe poner en riesgo los equipos y estaciones de trabajo con alimentos y bebidas que puedan causar daño o deterioro. Para esto se debe hacer la señalización adecuada en la cartera de ONAC y pieza informativa al personal interno.
- Garantizar el aseo y mantenimiento adecuado de los equipos asignados a su cargo.
- Los usuarios no deben instalar programas o aplicaciones en las estaciones de trabajo. Toda instalación o cambio en la configuración debe realizarse con la autorización y responsabilidad del área de TI
- Se prohíbe totalmente modificar o intentar hacer cambios en la configuración de seguridad del equipo. El incumplimiento de esta política se considera falta grave.
- Las actividades de mantenimiento del equipo solo pueden ser realizadas por el personal de TI o por el proveedor.
- El usuario no debe desmontar partes o componentes tanto de software como de hardware para reemplazo sin la solicitud de soporte al área de gestión de TI.
- El usuario no debe dar acceso al equipo a terceros no autorizado
- El respaldo de la información almacenada en el disco duro de una estación de trabajo estará en los servidores, TI se encarga del respaldo de estos.
- El uso de carpetas compartidas sólo será para información empresarial.
- Se debe desconectar el equipo de la red cuando se detecte un virus o exista sospecha de un virus y avisar de inmediato al área de gestión de TI.
- Cuando el usuario no cuente con una estación de trabajo asignada u operativa, no está autorizado para utilizar equipos portátiles personales para actividades laborales sin autorización del encargado de área de TI..

8.5 Requisitos de seguridad para equipos móviles

Los equipos que sean utilizados fuera de las instalaciones deben ser objeto de controles de seguridad. Los controles incluyen:

- La entrega de equipos portátiles (que serán usados fuera de las instalaciones) debe ser expresamente autorizado, por correo electrónico, por el jefe inmediato, Coordinador de Gestión de TI y copia al Director Administrativo y Financiero.
- El equipo debe identificarse adecuadamente según el PR-5.5-01 Gestión de activos de Información y licenciamiento de forma visible y clara para prevenir hurto y facilitar la trazabilidad.
- El usuario del equipo es responsable de la seguridad del mismo por fuera de las instalaciones, por tanto, debe tener en cuenta los cuidados necesarios para evitar robo de equipos, información o daño del equipo.
- La conexión para trabajo remoto debe realizarse según el procedimiento de control de acceso con el servicio de VPN o el que se tenga dispuesto por el área de gestión de TI.
- Los usuarios no deben instalar programas o aplicaciones en equipos portátiles. Toda instalación o cambio en la configuración debe realizarse bajo responsabilidad de TI
- Se prohíbe totalmente modificar o intentar hacer cambios en la configuración de seguridad del equipo. El incumplimiento de esta política se considera falta grave.
- Las actividades de mantenimiento del equipo solo pueden ser realizadas por el personal de TI en las instalaciones de ONAC.
- El usuario no debe desmontar partes o componentes para reemplazo sin la solicitud de soporte al área de TI.
- El usuario no debe dar acceso al equipo a terceros no autorizados

8.6 Política de escritorio limpio y pantalla despejada

Los usuarios de los sistemas de información deben controlar el acceso no autorizado a la información manteniendo escritorio y pantalla despejados. Se considera equipo desatendido cuando el usuario se retira de su puesto de trabajo dejando su equipo activo y registrado en la red, dando la posibilidad de uso por un tercero no autorizado.

Esta situación genera un riesgo para la confidencialidad e integridad de la información que debe mitigarse aplicando los siguientes controles:

- Termine siempre la sesión cuando finalice su labor. No se limite a apagar el equipo, también debe cerrar la sesión en servidores cuando se trabaje en ellos.
- En caso de retirarse temporalmente del puesto de trabajo en sesión activa, mantenga activado el protector de pantalla con contraseña siguiendo recomendaciones dadas anteriormente.
- No deje información clasificada como confidencial sobre su escritorio ya sea en medio impreso (papel) o electrónico en medios de almacenamiento (USB o CD). Este tipo de información debe guardarse siempre bajo llave.

8.7 Uso de medios de almacenamiento y transporte de la información

Los medios de almacenamiento incluyen dispositivos USB, Discos, CD y DVD. Se deben cumplir los siguientes controles para su seguridad:

- Los medios removibles como CD, USB y otros deben mantenerse siempre bajo llave bajo responsabilidad del usuario.
- El contenido de todo medio re-utilizable, previamente a ser desechado, debe procesarse para hacerlo irrecuperable.
- Todo medio debe ser almacenado en un ambiente protegido y seguro, de acuerdo con las especificaciones del fabricante.
- Si el tiempo de almacenamiento de la información almacenada fuera mayor que el tiempo de vida de los medios de soporte deberán adoptarse previsiones para evitar pérdidas por degradación física.
- El uso de cualquier dispositivo extraíble (CD, DVD, USB) está restringido para información clasificada, de carácter privado y reservada de carácter personal los usuarios que requieran hacer uso de este deben solicitar autorización al director del área correspondiente y posteriormente acercarse al área de gestión de TI para efectos de vacunación del dispositivo.

8.8 Eliminación de equipos y medios de almacenamiento

Cuando cumplen con su vida útil o ya no sean requeridos los equipos y medios de almacenamiento, se debe eliminar de manera segura y efectiva, teniendo en cuenta:

- Los usuarios de los equipos no pueden realizar la eliminación de equipos o medios de almacenamiento. Esta responsabilidad es del área de gestión de TI, de acuerdo con las buenas prácticas ambientales orientadas al cuidado del medio ambiente.
- El Analista de TI debe comunicarse con la entidad encargada de la disposición segura de medios y equipos de este tipo para la conservación del medio ambiente para la eliminación.
- Los medios y equipos que contienen información sensible deben ser almacenados y eliminados de manera segura y efectiva, ya sea mediante incineración, destrucción o borrado de datos para ser utilizados por otra aplicación.
- Cuando se trata de equipos adquiridos por sistemas de renta, se debe hacer eliminación total de la información y las aplicaciones instaladas previo a su devolución al proveedor.
- La eliminación de información en equipos y medios y su posterior destrucción o devolución debe soportarse mediante un acta.
- No se debe dejar acumular información o equipos para su eliminación posterior. La eliminación segura debe realizarse de forma inmediata.

9. SERVICIOS DE TECNOLOGÍA DE LA INFORMACIÓN

9.1 Accesos y privilegios

las políticas de seguridad de la información dirigidas a los usuarios con relación a los accesos a los servicios y aplicaciones son las siguientes:

- Los accesos a los servicios de procesamiento de información al igual que las aplicaciones empleadas en las actividades laborales de ONAC, son asignadas de acuerdo a los roles establecidos para cada uno de los cargos de acuerdo con la matriz de accesos y privilegios del procedimiento PR-5.5-03 Gestión de acceso.
- Los accesos y privilegios dentro de los servicios de tecnología y aplicaciones de ONAC son asignados por el área de gestión de tecnologías de la información por solicitud de gestión humana para el caso del personal interno, por solicitud de gestión de competencias para evaluadores y expertos técnicos o contratistas por el supervisor del contrato.
- No es permitido el acceso a aplicaciones o servicios de tecnología que no se encuentren definidos para el rol del cargo o que se hayan autorizado de manera explícita y por las direcciones de ONAC
- El acceso a aplicaciones o servicios para las cuales no se tiene autorización se considera falta grave e incumplimiento de las políticas de seguridad de la información
- En caso de detectar que se tiene acceso alguna aplicación o servicio para la cual no se está autorizado se debe informar al área de tecnología de la información para realizar la corrección necesaria

9.2 Uso de contraseñas (passwords)

El área de tecnología de la información establece y asigna un ID y una contraseña para el usuario nuevo en el sistema, quien debe seguir las siguientes directrices:

- Cambie la contraseña inicial segura de forma inmediata
- No escriba la contraseña en sitios no protegidos (archivos de papel, correo electrónico, medios removibles)
- No divulgue su contraseña
- Cambie la contraseña al menos una vez por mes o cuando se presenten incidentes de seguridad que lo ameriten
- No utilice contraseñas consideradas como no seguras evitando nombres (propio o de familiares), números de teléfono, fechas de cumpleaños, número de cedula).
- Es recomendable mezclar caracteres numéricos y alfanuméricos
- Evite usar secuencias como 12345678, ABCDEFGH, Admin123, ONAC123, Colombia00 o Nombre123
- No use contraseñas personales usadas para otras aplicaciones como cuentas de correos personales, bancarios u otras.
- Atienda las recomendaciones suministradas por TI sobre el uso de contraseñas.

9.3 Uso de Internet

El uso de navegación por Internet debe seguir las siguientes disposiciones:

- Solo tenga activado el navegador cuando esté haciendo uso del servicio. En caso de no estar usándolo cierre el programa para no consumir recursos del sistema.
- No es permitido suministrar información de la empresa en los grupos de discusión de Internet, redes sociales y otros sin previa autorización.
- No haga uso del servicio de Internet para fines diferentes a las actividades laborales
- No es permitido el uso de servicios de Internet para explorar paginas con contenidos ilegales, de acoso, difamatorio, abusivo, amenazador, nocivo, vulgar o de cualquier otra manera, censurable.
- No se permite la descarga e instalación de ningún tipo de programas o aplicaciones encontradas en Internet. Todo cambio en la configuración debe realizarse a través del área de gestión de TI.
- No se permite la descarga de contenidos fuera del alcance del objeto del trabajo como música, videos, juegos o películas.
- Deben respetarse siempre los requisitos de derechos de propiedad intelectual.
- No está permitido el acceso a redes sociales en el trabajo, salvo las autorizadas por el área de comunicaciones y Gestión de TI
- La conexión a Internet por parte de los empleados debe realizarse a través del perímetro protegido de la red LAN. El uso del Wi-Fi ONAC_INVITADOS es solamente para proveedores y visitantes.
- No es permitido suministrar la clave de acceso la red Wi-Fi ONAC_CORP a personas externas no autorizadas.
- No suministre información personal o empresarial en páginas de Internet que no sean autorizadas por el área de gestión de TI.
- El uso de servicios de mensajería instantánea, voz o video conferencia solo pueden utilizarse con la aprobación del área de gestión de TI.

9.4 Uso de correo electrónico

Para el uso del correo electrónico corporativo de ONAC, debe aplicar siguientes reglas de seguridad:

- El uso de la cuenta de correo y su contraseña son responsabilidad absoluta del usuario. Por tanto, su uso es personal e intransferible.
- Si recibe un mensaje con archivos adjuntos de dudosa procedencia no lo abra, elimínelo inmediatamente de todas las carpetas de su computador, incluyendo la papelera de reciclaje. Notifique al analista de gestión de TI para incluirlo en el control de Spam.
- Se prohíbe el envío de información confidencial a través de medios electrónicos
- La información clasificada como confidencial, es de uso interno y por ningún motivo puede ser enviada o publicada a personal que no sea autorizado.
- Por ningún motivo se puede transmitir a través del correo material ilegal, de acoso, difamatorio, abusivo, amenazador, nocivo, vulgar o de cualquier otra manera, censurable.
- No es permitido interrumpir el tiempo de trabajo de sus compañeros con mensajes de correo que no sean laborales, como: mensajes en cadena, oraciones a cambio de beneficios, chistes, videos o cualquier manifestación similar. Esto no sólo entorpece las labores diarias si no que además afecta la capacidad del servidor.
- Los mensajes enviados por el correo electrónico deben ser respaldados por el usuario y son datos de su responsabilidad.
- El usuario debe depurar permanentemente el correo debido a que el buzón tiene un tamaño limitado. No hacerlo puede ocasionar problemas en la recepción o envío de mensajes de toda la Compañía.
- Los correos transmitidos son correspondencia privada entre el destinatario y el remitente. Por tanto, cualquier conducta de intercepción, modificación, alteración o apropiación de mensajes, será considerado como falta grave.
- El usuario es el único responsable de los contenidos de sus correos enviados a través del correo electrónico.
- El usuario no debe crear una identidad, dirección o encabezamiento de correo electrónico falso o intentar engañar a otras personas con la identidad del remitente o el origen del mensaje.
- El correo se convierte en prueba legal y por tanto las autoridades competentes pueden usar este material como instrumento probatorio de cualquier hecho indebido.
- Si usted encuentra un mensaje que rompa las leyes de la conducta del usuario del correo electrónico, respeto o seguridad, por favor remitir el mensaje a la cuenta de correo del Coordinador de TI.
- No se debe anexar archivos, enviar páginas web o contenidos de la empresa sin la debida autorización.
- Abstenerse de enviar correos electrónicos empresariales desde correos electrónicos personales y gratuitos porque esto ocasiona envío de SPAM al correo electrónico.

Recomendaciones adicionales para el uso del correo:

- Revise diariamente su correo y responda oportunamente sus mensajes.
- Informe a su interlocutor si va a suspender la comunicación por algún motivo (vacaciones, viajes de trabajo).
- El lenguaje usado en las comunicaciones de trabajo debe ser formal. La informalidad en el lenguaje disminuye la seriedad y credibilidad de la información a transmitir.
- El contenido de los mensajes debe ser conciso. Es recomendable tratar un solo tema, esto contribuye a su comprensión y manejo
- Escriba de manera sencilla, clara y corta, lo que evita la pérdida de tiempo al lector y además ahorra tiempo de conexión. Evite la letra de difícil lectura.
- Evite el uso de abreviaturas o expresiones poco usuales para el destinatario del mensaje
- El uso de mayúsculas sostenidas en el correo electrónico no es recomendable, tanto para la descripción del asunto como para el contenido. Esto es interpretado como un llamado de atención.
- Relea su mensaje antes de enviarlo, aunque sea un sistema más informal que una carta, los puntos y las ideas deben ser claros. Igualmente debe verificarse la digitación, presentación, ortografía y puntuación.
- Antes de enviar un correo electrónico verifique si la dirección escogida en la libreta de direcciones es la correcta.
- Al reenviar un mensaje, ponga sus propios comentarios al principio, no al final. Esto le permite a la persona que lo recibe conocer con anterioridad el propósito de su correo.

Al escribir un correo electrónico tenga en cuenta los siguientes lineamientos:

- Definición del asunto: el asunto debe estar claramente definido en cada uno de los correos emitidos. Debe ser corto y muy puntual.
- El contenido de los mensajes: debe ser corto, los textos extensos deben anexarse, teniendo en cuenta primero el peso del archivo. Los anexos deben contener solamente información que sea útil y necesaria.
- Envío de copias: se debe hacer participe de la información sólo a aquellas personas que tengan relación con el tema y no de manera indiscriminada a todo el personal.
- Establecer una plantilla única de correo, aplicar a la firma lo siguiente: cada mensaje que se envíe debe ir firmado por la persona que lo emite (nombre, cargo, área, teléfonos y dirección de la empresa).

9.5 Políticas generales

Ingeniería social:

Se deben aplicar las siguientes buenas prácticas de seguridad de la información para evitar ataques de ingeniería social que puedan afectar los sistemas de información de ONAC:

- Tenga en cuenta que los ataques de ingeniería social son diseñados para aprovechar rasgos humanos como la curiosidad, el respeto por la autoridad y el deseo de ayudar.
- Verifique la fuente de los mensajes que considere sospechosos, como direcciones de correo o enlaces
- No actúe de forma precipitada para responder o reenviar información sospechosa. Confirme en las paginas oficiales de entidades supuestamente que envían la información antes de tomar decisiones
- Confirme si de trata de una situación realista, analizando la posibilidad de que se trate de un tema real o fraudulento
- No utilice la misma contraseña pata diferentes servicios o aplicaciones. Si su contraseña ha quedado expuesta cámbiela de forma inmediata

9.6 incumplimiento y procesos disciplinarios

El incumplimiento de estas políticas de seguridad de la información traerá consigo las consecuencias legales que apliquen al RRI-5.4-01 Reglamento Interno de Trabajo v3, incluyendo las sanciones que se establezcan en las normas que competen al Gobierno Nacional y Territorial en cuanto a seguridad y privacidad de la información se refiere.

10. REGISTROS (Documento Evidencia)

Código	Nombre	Almacenamiento Físico	Almacenamiento Magnético
N/A	**N/A**	N/A	N/A

11. CONTROL DE CAMBIOS

Versión	Fecha de Aprobación	Resumen de Cambios
01	2023-02-28	Versión inicial del documento

12. ANEXOS

N/A