NEORIS

Título: Resumen de la Política de Seguridad de Información y Ciberseguridad de NEORIS

Tipo de Documento: Resumen de Política	**ID:** CYB-PO-GLO-11
Área Funcional: Seguridad de Información	**Fecha de elaboración:** Oct-2024
Ubicación: Global	**Fecha de entrada en vigor**: Oct-2024
Versión: 1.0	

1 Historial de Revisiones

Versión	Fecha	Autor	Revisor	Aprobador	Cambios
1.0	Sept, 2022	Daniel Mijares	Sebastian Manzanares Rafael Zamora	Verónica Mancho (CIO) Daniel Ramirez (CISO)	• Creación del resumen basado en la Política de Seguridad de Información y Ciberseguridad.

www.neoris.com
1395 Brickel Avenue, Suite 500
Miami, FL 33131, EE.UU.

/neoris
/neoris.corporate
/company/neoris
/neoris_global

2 Tabla de Contenido

www.neoris.com
1395 Brickel Avenue, Suite 500
Miami, FL 33131, EE.UU.

/neoris
/neoris.corporate
/company/neoris
/neoris_global

3 Objetivo

El Objetivo de este documento es proporcionar un resumen de la Política de Seguridad de la Información y Ciberseguridad, para que sea más fácil conocer sus principales directrices.

4 Alcance y Aplicabilidad

Este documento es aplicable a la Corporación NEORIS, sus regiones, países, empresas afiliadas y sus empleados, contratistas, proveedores, consultores y socios comerciales.

5 Roles y Responsabilidades

- Gerencia: La gerencia promoverá las políticas de NEORIS y deberá proporcionar un primer nivel de supervisión a los empleados.
- Los empleados de NEORIS deberán obedecer las políticas de NEORIS.

6 Organización de la Seguridad

- La seguridad de la información es responsabilidad de cada empleado. Los empleados deberán cumplir con todas las políticas, procedimientos y estándares de seguridad.
- Los "Dueños de Procesos de Negocio" son responsables de la Seguridad de la Información de sus propios procesos y activos de información.
- Las Áreas Comerciales y Áreas de Entrega de Servicios (de cada Digital) son responsables de la definición del nivel de seguridad y privacidad a incluir en los Servicios. Las Áreas de Entrega de Servicios son responsables de establecer y mantener el nivel de seguridad y privacidad de acuerdo a la definición inicial. Se recomienda que se asigne el rol de Coordinador de Privacidad y Seguridad del Servicio para garantizar el cumplimiento.
- El **Equipo de Seguridad de la Información** es responsable de gestionar todas las iniciativas de seguridad de la información de NEORIS a nivel corporativo de Business Support.

7 Control y Clasificación de Activos

- Las áreas de NEORIS elaborarán y mantendrán un inventario de todos los activos de información sensible.
- Las áreas de Entrega de Servicios deberán contar con un inventario de activos de información relacionada a clientes o proyectos.
- Toda la información será clasificada utilizando las siguientes categorías de acuerdo a la política de Clasificación de Información:
    a) No de Negocio
    b) Público
    c) Uso Interno
    d) Confidencial
    e) Restringida

www.neoris.com
1395 Brickel Avenue, Suite 500
Miami, FL 33131, EE.UU.

/neoris
/neoris.corporate
/company/neoris
/neoris_global

- El propietario de los activos deberá revisar periódicamente la clasificación asignada a todos los activos de información sensible para garantizar su coherencia y validez.
- Las etiquetas de los activos de información serán revisadas por el propietario de la empresa al menos una vez al año para comprobar su idoneidad.

8 Seguridad del Personal

- Las responsabilidades de Seguridad de la Información deberán documentarse en las descripciones de trabajo.
- Los empleados de NEORIS deberán firmar un Acuerdo de Confidencialidad como parte de sus términos y condiciones iniciales de empleo.
- Los contratistas y otros terceros que trabajen para NEORIS o Cliente de NEORIS también deberán firmar un Acuerdo de Confidencialidad.
- Los términos y condiciones de empleo deberán indicar: "El cumplimiento de la política de seguridad de la información de NEORIS es obligatorio". Cualquier incumplimiento de esta o cualquier otra política de seguridad puede resultar en medidas disciplinarias que pueden incluir el despido inmediato de NEORIS y un posible procesamiento bajo leyes locales, estatales y federales aplicables".
- Todos los empleados de NEORIS y usuarios externos recibirán capacitación adecuada y actualizaciones periódicas en políticas y procedimientos de seguridad de la información.
- Se aplicará una **prueba de seguridad** a todos los empleados de NEORIS, con el fin de reforzar la concienciación de la Política de Seguridad y las responsabilidades de los usuarios.
- Todas las actividades sospechosas relacionadas con violaciones de seguridad de la información deben informarse a: la **Comisión de Ética** para garantizar un trato correcto y justo a los empleados sospechosos de haber cometido violaciones de seguridad graves o persistentes y al **Dueño de Proceso de Negocio**.
- Cualquier empleado o usuarios terceros declarados culpables de cualquier violación a la seguridad de la información podrán ser separados de sus funciones.

9 Respondiendo a Incidentes de Seguridad y Malfuncionamientos

- Los empleados o contratistas de NEORIS deberán reportar cualquier incidente de seguridad o posibles incidentes de seguridad de inmediato a la herramienta de seguridad de TI https://itsecurity.neoris.net, a la mesa de ayuda Help Desk o a itsecurity@neoris.com.
- Los incidentes de seguridad que involucren Datos Personales serán notificados al Delegado de Privacidad de Datos, DPO. Es importante que la notificación se realice dentro de las primeras 24 horas.
- Deberá existir un Plan de Respuesta a Incidentes de Ciberseguridad para gestionar los incidentes de seguridad.
- Si un incidente de seguridad afecta las operaciones de un cliente de NEORIS, se notificará el incidente de seguridad al punto de contacto designado por el Cliente de conformidad con el contrato.
- Las Áreas de Entrega de Servicios son responsables de realizar las notificaciones al cliente, de acuerdo con el asesoramiento profesional de Legal y del Equipo de Ciberseguridad. Las Áreas de Entrega de Servicios son responsables de gestionar los incidentes de seguridad internamente en los equipos de Entrega de Servicio de NEORIS con los clientes.

www.neoris.com
1395 Brickel Avenue, Suite 500
Miami, FL 33131, EE.UU.

/neoris
/neoris.corporate
/company/neoris
/neoris_global

- El Coordinador de Seguridad y Privacidad del Servicio se incorporará al equipo de respuesta de Ciberseguridad para brindar conocimiento profundo sobre el Servicio, su infraestructura, las responsabilidades de NEORIS y gestionar internamente cualquier problema con el equipo de entrega del servicio.

10 Seguridad Física y Ambiental

- Todas las oficinas de NEORIS estarán protegidas por controles de entrada adecuados para garantizar que sólo se permita el acceso al personal autorizado.
- Los departamentos o áreas con requisitos de seguridad adicionales deberán definir áreas seguras para agregar mecanismos de seguridad para proteger sus activos de información.
- Las instalaciones/áreas seguras deberán estar protegidas y monitoreadas mediante controles apropiados para garantizar un nivel adecuado de seguridad.
- Los usuarios deben bloquear la pantalla de su computadora cuando estén temporalmente lejos de su escritorio.
- Cada empleado es responsable de minimizar el riesgo de robo de todos los recursos informáticos personales y dispositivos de NEORIS asignados (por ejemplo, computadoras de escritorio y portátiles).
- Los empleados no deben conectar su propio equipo a la red NEORIS o a las instalaciones de información. Solo se permiten teléfonos celulares en un esquema BYOD si están debidamente inscritos en la Gestión de NEORIS.

11 Gestión de la Operación y de las Comunicaciones

- Los procedimientos operativos especificarán las instrucciones para la ejecución del trabajo y deberán ser revisados anualmente por el propietario.
- Se establecerá un proceso de Gestión de Cambios para regir los cambios en la infraestructura tecnológica.
- Se deben separar deberes y áreas de responsabilidad para minimizar el riesgo de fraude y errores en el procesamiento de información, transacciones o información o servicios.
- Los Dueños de Procesos de Negocio son responsables de establecer una adecuada segregación de funciones.
- Antes de utilizar servicios externos de gestión de instalaciones, se identificarán los riesgos y se acordarán con el contratista los controles adecuados y se incorporarán al contrato.
- La planificación de la capacidad para los sistemas de procesamiento de información y activos de información críticos se realizará anualmente.
- Se evitará que nuevos sistemas ingresen al entorno de producción hasta que los propietarios del sistema hayan revisado y autorizado los resultados de la prueba de aceptación.
- Cada equipo de usuario final deberá contar con el software antivirus autorizado. Este se deberá actualizar automáticamente.
- Los escaneos de vulnerabilidad se deberán realizar periódicamente, al menos uno por trimestre; se recomienda encarecidamente realizar análisis mensuales.
- Se deberán realizar copias de seguridad de la información y el software empresarial críticos con regularidad.
- Las bitácoras generadas automáticamente mantendrán la actividad del sistema.

www.neoris.com
1395 Brickel Avenue, Suite 500
Miami, FL 33131, EE.UU.

/neoris
/neoris.corporate
/company/neoris
/neoris_global

- Los usuarios en ubicaciones remotas deberán utilizar una red privada virtual (VPN) y autenticación MFA para salvaguardar la confidencialidad y la integridad de los datos que pasan a través de redes públicas.
- El acceso a la red de NEORIS deberá estar protegido por tecnología NAC, que solo permitirá el acceso a dispositivos y usuarios autorizados cumpliendo con los controles de seguridad.
- El almacenamiento de información sensitiva en medios extraíbles está prohibido para los usuarios normales. Solo el personal de TI en el desarrollo de sus funciones administrativas puede almacenar información sensible en medios extraíbles.
- El correo electrónico se utilizará para fines autorizados por NEORIS.
- Los mensajes de correo electrónico son propiedad de NEORIS.
- En las oficinas de NEORIS sólo se utilizará la red inalámbrica oficial de NEORIS.
- Para el acceso remoto desde un punto de acceso inalámbrico público se deberá usar VPN.
- Los empleados protegerán el intercambio de información utilizando únicamente las comunicaciones oficiales gestionadas por NEORIS.
- Los empleados no deberán discutir información confidencial en áreas públicas, transporte público.
- El uso del altavoz del teléfono para discutir información confidencial está restringido a áreas cerradas.
- Los documentos de las impresoras o fotocopiadoras se deben retirar con prontitud y nunca se deben dejar desatendidos en las bandejas.

12 Control de Accesos

- El acceso a los sistemas NEORIS debe proporcionarse mediante autenticación Multi-factor MFA.
- Se establecerá una identificación de usuario única para que se puedan rastrear las actividades del usuario.
- Los usuarios se verán obligados a cambiar la contraseña en la primer sesión para garantizar la confidencialidad de la contraseña.
- La contraseña debe cambiarse cada 60 días de acuerdo con la Política de Contraseñas de NEORIS.
- Los derechos de acceso del usuario serán revisados por el Dueño del Proceso de Negocio al menos casa 6 meses.
- Los equipos desatendidos deberán estar física y lógicamente bloqueados. Es decir, bloqueo de pantalla, cierre de sesiones.
- El acceso a la red de NEORIS deberá estar protegido por tecnología NAC, que solo permitirá el acceso a dispositivos y usuarios autorizados cumpliendo con los controles de seguridad.
- En la Infraestructura tecnológica de NEORIS solo se permiten dispositivos de usuario final propiedad de NEORIS y dispositivos de terceros autorizados.
- El acceso a la Información y a Aplicaciones estará restringido a usuarios autorizados de acuerdo con los requerimientos del Dueño de Proceso de Negocio.
- Se requiere Gestión de Acceso Privilegiado para la infraestructura critica de Sistemas de Información Corporativa de NEORIS.
- Las tecnologías SIEM se deben utilizar para proteger aún más la infraestructura de NEORIS.

www.neoris.com
1395 Brickel Avenue, Suite 500
Miami, FL 33131, EE.UU.

/neoris
/neoris.corporate
/company/neoris
/neoris_global

13 Mantenimiento y Desarrollo de Sistemas

- Se deberá implementar un Proceso de Desarrollo de Software Seguro para los Clientes NEORIS y para desarrollos internos.
- Al desarrollar Sistemas de Información se deberá realizar un análisis de los requerimientos de seguridad y privacidad
- La idoneidad de los requerimientos de seguridad de la información y de la privacidad serán resueltas por el Dueño del Proceso del Negocio y el Arquitecto de Seguridad del Proyecto.
- Se deberán realizar validaciones de seguridad al código de Software, tanto validación estática como dinámica, y se deberán resolver las deficiencias encontradas antes de implementar el sistema en el entorno de producción.
- Se deberá utilizar cifrado robusto para proteger las comunicaciones y la información altamente sensible, como la información de identificación personal.

14 Gestión de la Continuidad del Negocio

- Se deberán desarrollar planes de continuidad para mantener o restaurar las operaciones de negocio de manera oportuna después de la interrupción o falla de los procesos críticos de negocio.
- Para todos los Escenarios Catastróficos que requieran Tratamiento de Riesgos, se establecerán estrategias de recuperación de Continuidad.
- Los planes de continuidad del negocio se deberán probar una vez al año o cada vez que se haya producido un cambio importante para garantizar que estén actualizados y sean efectivos.

15 Cumplimiento

- El Departamento Legal asesorará a NEORIS sobre todos los requisitos regulatorios relacionados con la seguridad y privacidad de la información para garantizar que no haya conflicto entre la legislación de cada país y las directivas de seguridad de la información definidas en esta Política.
- Todos los empleados deberán firmar el "Acuerdo de Confidencialidad y Derechos de Propiedad Intelectual" como parte del proceso de contratación.
- Todos los Consultores y terceros deberán firmar el "Acuerdo de Confidencialidad y Derechos de Propiedad Intelectual" antes de trabajar para NEORIS.
- Todas las estaciones de trabajo utilizadas para fines de negocio de NEORIS deberán ser contar con licencia de software.
- Las licencias de software de todos los productos de software serán controladas y mantenidas por el Departamento de Tecnología de la Información.
- Recursos Humanos sigue comprometido a proteger la privacidad y confidencialidad de la información de sus Empleados. Establece prácticas uniformes para recolectar, usar, divulgar, almacenar, acceder, transferir o procesar de otro modo la información.

www.neoris.com
1395 Brickel Avenue, Suite 500
Miami, FL 33131, EE.UU.

/neoris
/neoris.corporate
/company/neoris
/neoris_global

16 Gestión de Riesgos de la Seguridad de Información

- La Gestión de Riesgos de Seguridad de la Información aplica a toda la infraestructura y los procesos de negocio de NEORIS. Los Dueños de Procesos de Negocio son responsables de la evaluación de riesgos de su propio proceso de negocio.
- Las Áreas de Entrega de Servicios deberán realizar una evaluación de riesgos de seguridad de la información si así lo exigen sus propios procesos, es parte del compromiso o contrato de servicio con el Cliente.
- El Equipo de Seguridad TI deberá realizar evaluaciones de riesgos en la Infraestructura corporativa, así como en el alcance del Sistema de Gestión de Seguridad y Privacidad de la Información, SGSPI.

17 Seguridad en la Nube

- Se definirá y comunicará una política específica de Seguridad en la Nube para establecer las bases de un marco de seguridad en la nube adecuado.
- Todas las áreas técnicas de NEORIS como TI y todas las Digitales deben cumplir con la Política de Seguridad de la Nube, así como el Dueño del Proceso de Negocio y el Propietario del Servicio que utilizan la Nube.
- NEORIS puede utilizar un sistema en la nube, pero siempre debe tener evidencia de la seguridad del Servicio en la Nube. Ejemplo de esta evidencia podrían ser Certificados ISO 27001, ISO27701, Reportes Tipo SOC, contratos, entre otros.

www.neoris.com
1395 Brickel Avenue, Suite 500
Miami, FL 33131, EE.UU.

/neoris
/neoris.corporate
/company/neoris
/neoris_global