SEGURIDAD NUEVA ERA LTDA., es una compañía comprometida con la seguridad de la información, para lo cual establece compromisos y un esquema de protección de datos. en la prestación de los servicios de vigilancia y seguridad privada en las modalidades de vigilancia fija, móvil y escolta a personas, vehículos y mercancías con utilización de armas de fuego y sin armas; el uso de medios tecnológicos y el servicio conexo de asesoría, consultoría e investigación en vigilancia y seguridad privada.

La presente política tiene como objetivo establecer las disposiciones que permitan crear una cultura de seguridad, confianza. Previniendo riesgos de accesos no autorizados, perdidas, daños de la información, dentro o fuera del horario normal, para lo cual su compromiso está enmarcado en las siguientes directrices:

DISPOSITIVOS MOVILES.

- Definir las responsabilidades explícitas para implementar, operar y administrar los controles de seguridad de la información.

- El proceso de seguridad electrónica e informática debe establecer las configuraciones aceptables para los dispositivos móviles corporativos o personales que hagan uso de los servicios provistos por SEGURIDAD NUEVA ERA LTDA.

- El proceso de seguridad electrónica e informática debe establecer un método de bloqueo (por ejemplo, contraseñas, biométricos, patrones, reconocimiento de voz) para los dispositivos móviles corporativos 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 requerir á el método de desbloqueo configurado.

- El proceso de seguridad electrónica e informática debe activar la opción de cifrado de la memoria de almacenamiento de los dispositivos móviles corporativos haciendo imposible la copia o extracción de datos si no se conoce el método de desbloqueo.
- La información restringida de SEGURIDAD NUEVA ERA LTDA no debe ser almacenada en dispositivos móviles. Sin embargo, en el caso de que no haya alternativa y el funcionario requiera almacenarla en un dispositivo móvil para su transporte, deben seguir las siguientes acciones de carácter obligatorio:

    1. Activar el cifrado de los datos en el dispositivo móvil y a continuación almacenar la información a ser transportada.
    2. Borrar la información del dispositivo móvil en el momento que ya no se requiera su almacenamiento en éste.
    3. Si es una memoria USB o disco duro externo, el transporte de información restringida, se debe realizar mediante contenedores o espacios cifrados.

- Asignar equipos y planes de telefonía celular para los colaboradores de acuerdo con las responsabilidades consignadas en el perfil del cargo.

- En caso de que el equipo soporte conexión vía bluetooth, se deben proteger estas conexiones mediante contraseña y haciendo que esta no se encuentre visible a todos los equipos. Evite enviar información restringida a través de correo electrónico, pero en el caso de que sea estrictamente necesario cifre el correo.

- Se debe instalar un software de antivirus tanto en los dispositivos móviles corporativos como en los personales que hagan uso de los servicios provistos por SEGURIDAD NUEVA ERA LTDA.

CONTROL DE ACCESOS.

Genera los controles para reducir los riesgos asociados a la seguridad de la información asociados al control de acceso físico a las instalaciones.

- Todos los sistemas de seguridad física deben cumplir con todas las regulaciones establecidas por la alta dirección.
- Todo acceso físico a las instalaciones por sus partes interesas será restringido, debiéndose gestionar y documentar de acuerdo a los protocolos establecidos para dicho fin.
- Las tarjetas de acceso magnético o claves de acceso a los sistemas de información NO deben ser compartidas o cedidas a otros.
- Las tarjetas de acceso magnético o claves de acceso que ya no sean necesarios o ya cumplieron su función, deberán ser devueltos al procesos de seguridad electrónica e informática. Las tarjetas no deberán ser reasignadas a otra persona sin pasar por el proceso de re enrolamiento.
- La pérdida o robo de las tarjetas de acceso magnéticas o claves deberán ser reportados al proceso de operaciones y seguridad electrónica e informática, al correo operaciones@seguridadnueveera.com, incluyendo en el mensaje los siguientes datos: Nombre completo del funcionario, dependencia, circunstancias en las cuales sucedió el robo o pérdida y copia de constancia de pérdida y/o elementos.
- Los registros de acceso de las tarjetas de acceso magnético o claves, deberán conservarse para mantener una revisión de los accesos y rutinas realizadas basadas en la criticidad de los recursos que se protegen.
- El procesos de seguridad electrónica e informática, en colaboración con el área de operaciones, serán los encargados de recuperar y eliminar los accesos a los lugares restringidos de las personas que sean desvinculadas o que por cambios en el contrato, cambien sus roles operativos.

- Los visitantes deberán ser escoltados por funcionarios internos o personal de seguridad en el acceso a las zonas controlas por las instalaciones.
- Los visitantes deben portar en un lugar visible la escarapela asignada por el área de operaciones, en el momento de ingresar a las instalaciones.
- Los funcionarios de SEGURIDAD NUEVA ERA LTDA. Al observar personal externos deambulando en las instalaciones deben direccionarlo al visitante hasta el lugar enunciado en su memento de ingreso, verificando la escarapela.
- El área de seguridad de la Información, se encargará de revisar periódicamente los privilegios y derechos de acceso de las tarjetas de acceso magnético o claves, para eliminar las de las personas que ya no requieran de éstos privilegios.
- El personal que ingrese los fines de semana por temas laborales, deben solicitar autorización al director de operaciones (operaciones@seguridadnueveera.com).
- Los funcionarios de SEGURIDAD NUEVA ERA LTDA. No pueden permanecer después de las 19:00 horas en las instalaciones, previo conocimiento del director de operaciones. Notificando la necesidad al correo electrónico operaciones@seguridadnueveera.com

PERSONAL AUTORIZADO.

El acceso al racks y la central de monitoreo estarán restringidos sólo al personal del proceso operaciones y de seguridad electrónica e informática. Los otros accesos a personal de servicios y demás partes interesas estarán restringidos, excepto previa autorización por parte del director de operaciones.

CONTROLES CRIPTOGRÁFICOS.

Controles con el objetivo de proteger la confidencialidad, autenticidad o integridad de la información mediante la ayuda de técnicas criptográficas.

- Las organizaciones deberían utilizarán controles criptográficos para la protección de claves de acceso a sistemas, datos y servicios, para la transmisión de información clasificada y/o para el resguardo de aquella información relevante en atención a los resultados de la evaluación de riesgos realizada por la organización.
- Sería necesario el desarrollo adicional de procedimientos y asignación de funciones respecto de la administración de claves, de la recuperación de información cifrada en caso de pérdida, compromiso o daño de las claves y en cuanto al reemplazo de las claves de cifrado.
- El uso de algoritmos de cifrado (simétricos y/o asimétricos) y las longitudes de clave deberían ser revisadas periódicamente para aplicar las actualizaciones necesarias en atención a la seguridad requerida y los avances en técnicas de descifrado.

- Las firmas digitales proporcionan un medio de protección de la autenticidad e integridad de los documentos electrónicos y, en algunas ocasiones, podría ser necesario asesoramiento legal para establecer acuerdos especiales que respalden su uso.
- Las claves de los usuarios dispondrán de un periodo no superior a noventa días, al terminar dicho tiempo el computador asignado al funcionario automáticamente exigirá al su modificación.
- En caso de olvidar la clave se reportara al proceso de seguridad electrónica e informática la pérdida, a fin de activar las medidas necesarias preventivas como correctivas.
- Implementar controles criptográficos con base en una evaluación de riesgos que identifique el nivel de protección necesario, teniendo en cuenta el tipo, la fortaleza y la calidad del algoritmo de cifrado requerido.

ESCRITORIOS LIMPIOS Y PANTALLAS LIMPIAS.

- Toda vez que un usuario se ausente de su lugar de trabajo, debe garantizar el bloqueo automático del equipo asignado, al mismo tiempo debe resguardar en su gabinete la documentación confidencial bajo llave.

- Al finalizar la jornada los funcionarios no deben dejar en sus escritorios información confidencial, sensible o clasificada, memorias, C.D, Post-it, entre otros dispositivos de almacenamiento de información.

- Los funcionarios de la compañía no deben abandonar u olvidar en sus escritorios, documentación personal, celulares, avénteles, radios, entre otros medios de comunicación.

- No se debe ingerir alimentos o bebidas cerca de los equipos o dispositivos de procesamiento de información, así como manipular líquidos en su cercanía, excepto los recipientes autorizados.

- Los funcionarios deben cerrar los cajones y gabinetes cuando se aleja del escritorio por periodos extendidos de tiempo.

- En caso de pérdida de las llaves de los escritos se debe notificar inmediatamente al personal de operaciones.

- Todos los equipos de cómputo y equipos portátiles deben tener el estándar aplicado relativo al protector de pantalla definido por el proceso de seguridad electrónica e informática.

- Cuando se reciban visitas de personal externo, no se deberá dejar expuesta información restringida a la vista de las personas ajenas, ni permitir su conocimiento sin autorización durante entrevistas, reuniones, entre otros.

- Todos los funcionarios son responsables de cerrar sesión al terminar su jornada de trabajo, evitando que los equipos de cómputo permanezcan activos.

- Los colaboradores deben de mantener los gabinetes de archivos cerrados con llave, evitando abandonarlas en sus cerraduras.

- Se debe Triturar el papel antes de arrojarlo.

- Se utilizara un sello de reciclaje al papel que por el contenido de su información puede hacerse uso en la parte posterior a la misma.

- Cuando sea aplicable, en los lugares donde se almacene información sensible, se debe implementar condiciones ambientales mínimas para el resguardo de los activos de la información, como temperatura y humedad, y deben ser monitoreadas.

- Los equipos de reproducción de información, como impresoras, fotocopiadoras, escáner, entre otros. Deben estar ubicados en lugares con acceso controlado y cualquier documento abandonado debe ser retirado de manera inmediata y reportar la novedad al área de operaciones.

- Capacitar a los usuarios en temas de seguridad.

TRANSFERENCIA DE INFORMACIÓN.

La información que circula en medios informáticos de SEGURIDAD NUEVA ERA LTDA. Durante su trasporte físico, debe estar protegida contra acceso no autorizado, uso inadecuado o corrupción. Se deben aplicar los siguientes controles.

- Para el traslado de información sensible o confidencial se deben usar transporte corporativo o mensajeros fiables, previo estudio de seguridad y proceso de selección estipulado.

- Los medios informáticos o de transporte físico de información del SEGURIDAD NUEVA ERA LTDA deben estar lo suficientemente protegidos contra daño físico que pueda ocurrir durante su transporte. Todo objeto a trasladar debe ser embalado y protegido correctamente con cajas de cartón y protectores de acopar para el caso de PC o servidores críticos, los objetos más delicados debe ir embalados con papel film industrial y/o huacas de madera de forma que se protejan contra golpes fuertes.

- Para él envió de documentos o paquetes se controlara con un código por proceso, que permita garantizar la trazabilidad del mismo.

- Los empleados de SEGURIDAD NUEVA ERA LTDA no deben revelar información sensible de sus proyectos por medios telefónicos, para evitar la escucha o interpretación de su llamada por personas extrañas.
- Los empleados de SEGURIDAD NUEVA ERA LTDA no deben mantener conversaciones confidenciales en lugares públicos y oficinas abiertas.

- No se deben dejar mensajes en contestadores automáticos que puedan reproducirse por personas no autorizadas.

- Al guardar información restringida de SEGURIDAD NUEVA ERA LTDA. En medios como celulares, tabletas y demás tecnologías móviles se deben activar las opciones de borrado remoto de la información almacenada en el dispositivo en caso de robo o pérdida del mismo, si éste las soporta.

- No se debe configurar reglas de reenvió de correos automático (respuesta instantánea) a correos externos.

- Implementar los controles necesarios para proteger los intereses de las partes interesadas de todo perjuicio ocasionado por fallas en la seguridad de la información.

DESARROLLO SEGURO.

- El proceso de seguridad electrónica e informática debe asegurase que los sistemas de información adquiridos o desarrollados por terceros, cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.
- El proceso de seguridad electrónica e informática debe asegurar que no se permitan conexiones recurrentes a los sistemas de información construidos con el mismo usuario.
- El proceso de seguridad electrónica e informática debe certificar la transmisión de información relacionada con pagos o transacciones en línea a los operadores encargados, por medio de canales seguros.
- Seguridad electrónica e informática debe generar metodologías para la realización de pruebas al software e información en general que contengan pautas para la selección de escenarios, niveles, tipos, datos de pruebas y sugerencias de documentación

RELACIÓN CON PROVEEDORES.

Garantizar la transparencia y fomentar la competitividad en el proceso de almacén, administrativo y financiero, generando condiciones de competencia abierta y justa entre los proveedores, asegurando igualdad de oportunidades.

- El personal encargado de interactuar en la adquisición de productos y servicios para SEGURIDAD NUEVA ERA LTDA, debe colocar órdenes de compra y celebrar contratos con proveedores sin incurrir en favoritismos de ninguna índole, privilegiando únicamente el interés global de la compañía.

- Cumplir con los procedimientos y políticas de compra definidos por el procesos de sistemas de gestión o que sean definidos por la Gerencia general para los distintos rubros específicos.

- Propender y promover estándares de calidad en los proveedores.

- Fomentar la integración operacional entre SEGURIDAD NUEVA ERA LTDA. y sus proveedores.

- Promover el desarrollo de proveedores y contratistas competitivos, a nivel local, nacional e internacional, apoyando e incentivando el emprendimiento.

- Formalizar acuerdos comerciales con proveedores, velando por el cumplimiento de las condiciones indicadas, en el marco de resguardar los intereses de ambas partes.

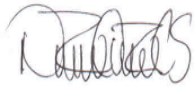
- Comprometer un tratamiento claro, abierto y oportuno en la resolución de conflictos con proveedores.

- Resguardar información confidencial atingente a SEGURIDAD NUEVA ERA LTDA y a sus clientes.

SANCIONES.

Cualquier incumplimiento a la presente política podrá dar a lugar al inicio de las acciones determinadas por SEGURIDAD NUEVA ERA LTDA. La infracción podrá constituir una violación a los principios de integridad, confidencialidad y disponibilidad de la información y será sancionada en conformidad a lo dispuesto GR-PR-07 PROCEDIMIENTO DISCIPLINARIO LABORAL. Lo anterior es sin perjuicio de la responsabilidad civil o penal que corresponda.

El proceso de seguridad electrónica e informática velará por el cumplimiento de estas políticas y sus respectivos controles, resguardando los intereses de SEGURIDAD NUEVA ERA LTDA, al mismo tiempo no se hará responsable por incidentes producidos por el no cumplimiento de estas políticas de seguridad.



NUBIA CASTRO.
Representante Legal.